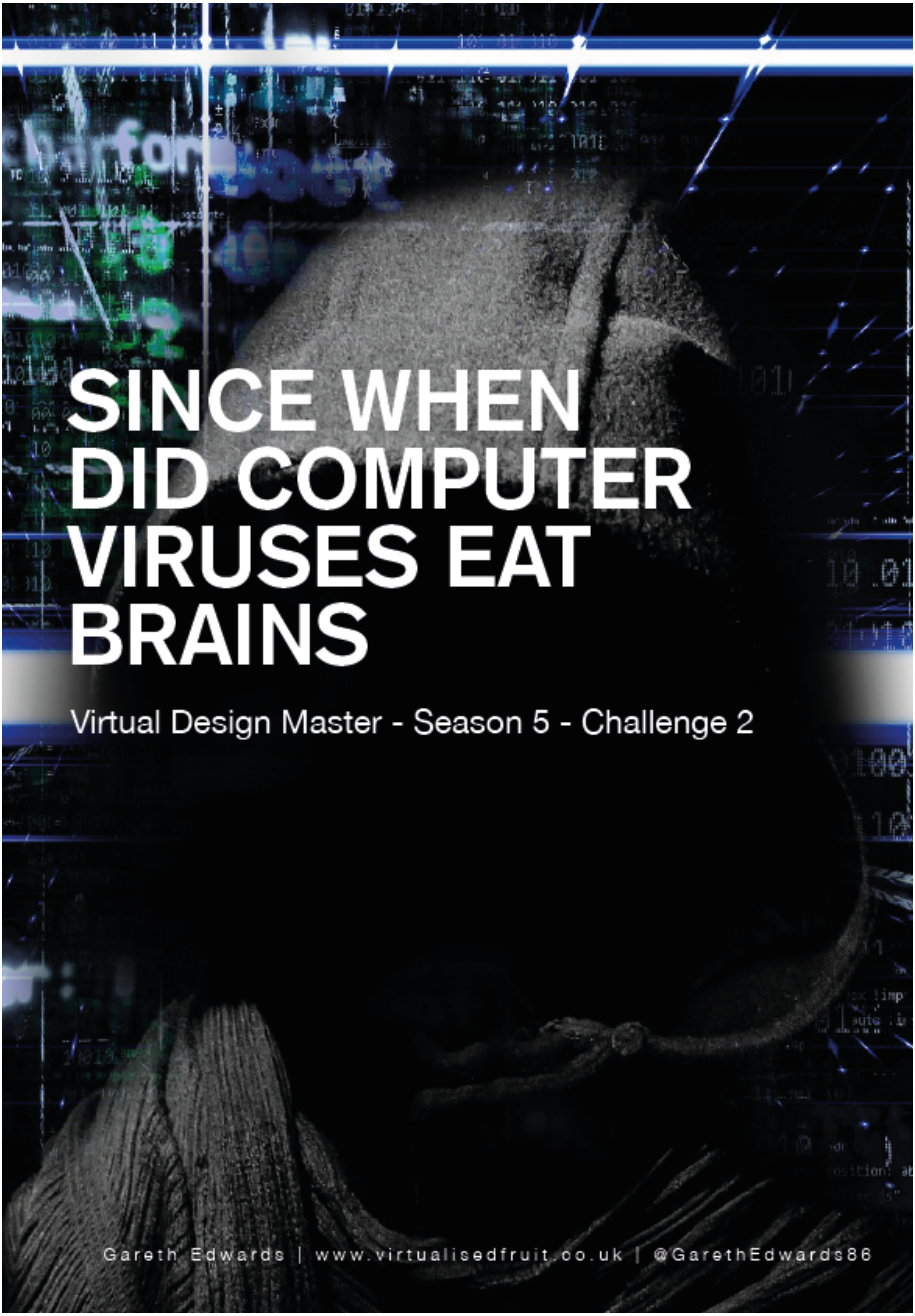


SINCE WHEN DID COMPUTER VIRUSES EAT BRAINS

Virtual Design Master - Season 5 - Challenge 2

Gareth Edwards | www.virtualisedfruit.co.uk | @GarethEdwards86

CHALLENGE 2

SINCE WHEN DID COMPUTER VIRUSES EAT BRAINS

TABLE OF CONTENTS

DOCUMENT CONTROL SHEET

Change Control

Customer Name	Virtual Design Master Challenge, Season 5	
Document Title	Challenge 2	
Version	V1.0	
Document Reference	Challenge 2 - Attack of the Zombie crypto.docx	
Project Reference	VDM Challenge 2	
Date of Creation	27 June 2017	
Date of Last issue	11 July 2017	
Author	Gareth Edwards	@GarethEdwards86

Distribution

Name	Position
Creative Panel	
Eric Wright	Creative Team
Melissa Wright	Creative Team / Deliverer of Evil??
Angelo Luciani	Creative Team
Judges	
Rebecca Fitzhugh	VCDX 243
Byron Schaller	VCDX 231
Lior Kamrat	VCDX 230

CHALLENGE 2

SINCE WHEN DID COMPUTER VIRUSES EAT BRAINS

Version Control

Version	Description of Change
0.1	Initial Creation
0.2	Final Revisions
1.0	Release to the world

Associated Documents

Title	Date	Source	Version
Season 4 – Challenge 1 – Back to Earth	01/07/2016	GitHub	1

Abbreviations

Abbreviations	Description
VPN	Virtual Private Network
VDM	Virtual Design Master
AI	Artificial Intelligence
DNS	Domain Name Services
DHCP	Dynamic Host Configuration Protocol
SMB	Server Message Block
DFS-R	Distributed File System Replication
AWS	Amazon Web Services
P2P	Point to Point
VM	Virtual Machine

CHALLENGE 2

SINCE WHEN DID COMPUTER VIRUSES EAT BRAINS

SYNOPSIS

You thought everything was running smoothly after you implemented the HumanityLink 2.0 software across the earth. It was, for a little while at least. Something has gone horribly wrong in the brand new infrastructure you have just implemented. The first site of your design from Challenge 1 has become infected with the EatBrains virus and ransomware which is now running rampant across your infrastructure. The EatBrains virus infects files and maps to SMB shares in order to spread itself further. There is also a variant that has the potential to store itself in memory on network devices and to emulate routers within the environment. EatBrains also has a phone home feature that allows for remote execution using the infected devices in the environment.

You must take your design from Challenge 1 and illustrate how you will accomplish the following:

1. Define how you will secure your infrastructure

2. Describe how you will find where the intruder has already breached and has remote execution capability

3. Create a recovery plan for every layer of the stack

4. Create a walk-through of how you will recover the HumanityLink application system which has been compromised

Be sure to include anything outside of this list that you think would thwart EatBrains in your environment.

Document submission is due Tuesday July 11th at 12 Midnight Eastern

CHALLENGE 2

SINCE WHEN DID COMPUTER VIRUSES EAT BRAINS

INTRODUCTION

Overview

We all knew it was coming but it appears that Zombie have manged to create a computer virus. So far it appears to be aggressive and may let our hacker back in from the previous series or has he been in our systems all along.

Intended Audience

This document is intended for the design board (our judges) to help make key decisions on implementing our new infrastructure.

Project Summary

I state this as a project summary but this time we are going to cover several scenarios as per the challenge document. I am also going to call out some of the weaknesses from my original submission and augment my design as needed during a recovery.

Project Requirements

The requirements of this project are to provide the design board with the following.

- Stop the EatBrains virus from spreading further
- Recover the Application
- Recover the Infrastructure
- Recover the network

CHALLENGE 2

SINCE WHEN DID COMPUTER VIRUSES EAT BRAINS

Project Assumptions

These are the assumptions we have made of this project is to provide the design board with the following.

- We assume in one of the scenarios that the antivirus failed and the virus managed to infiltrate our systems
- We can cover several scenarios to call out better designs, sometimes your best design can fail due to new security attacks.
- We have a CMDB with all our serials and MAC addresses
- We do not know if EatBrains can self-replicate or not
- We had SSH keys for routers and key network points before the attack

Project Constraints

The constraints of the project are outlined below.

- We may have lost data

Project Risks

The risks of this project are outlined below.

- There may be no known hot fixes available
- This may be a new variant able to bypass our current security systems

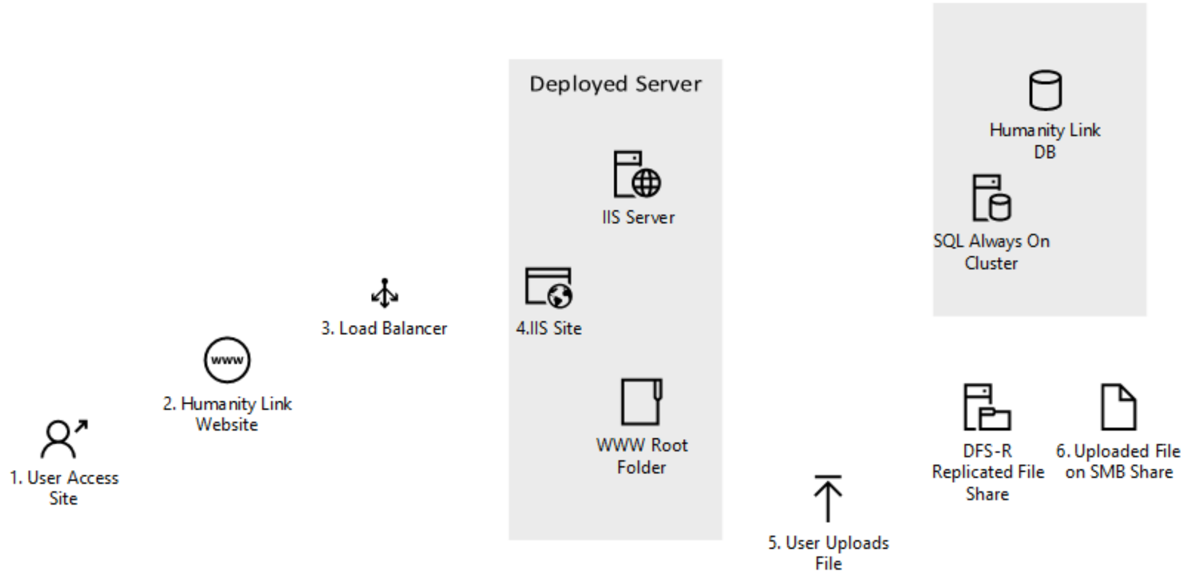
CHALLENGE 2

SINCE WHEN DID COMPUTER VIRUSES EAT BRAINS

SCENARIO AGNOSTIC POINTS

Application Delivery

With my previous design I did not take into account for the applications delivery or model. We have provided a very high level diagram into our application and its deployment along with its interactions with the other systems.



The application and servers are suggested to be deployed via (Terraform) and then for now using a PowerShell script to point the WWW virtual folder to a centralised SMB share to keep the code consistent for now. We know this is a risk but as the code should be backed up at least every hour (if not 15 minutes depending on recovery model) we feel this is adequate as we have not been provide any recovery time by our client. It is also anticipated that if an issue occurs a local copy may still be available on an engineers machine or in their GitHub Repro that isn’t on an SMB share. There is a view to eventually push this via GitHub to ensure change control as provide in an AWS Example by **clstokes** in his article (Deploy a Complex Infrastructure in AWS, 2016) but our engineers are recreating this code for our deployment so it also performs actions to our VMware environment and issues VMs to AWS. We also want to build some code in to configure the load balancers.

Backup Schedules

I found that I did not have enough time to cover this in the previous design but due to time constraints I want to cover how and why we may have deployed the backup jobs. The main Rubrik jobs we would have set to across 45 minutes of which each site being staggered with 15 minute intervals. We also assume that these jobs take less than 15 minutes to run and the reason for not having them all run at once is to try and provide a lower RPO if all sites are assumed as available.

The Nimble snapshots would then also take every 30 minutes to try and aid in recovery but these would need to not occur at the same time as the Rubrik snapshots to avoid clashing in VMware.

Finally the Veeam jobs would run at least hour if not more at the opposite time to the Nimble snapshots.

The tape jobs would only run daily to ensure there is a final copy of data on immutable storage to at least allow a worst case RPO of 24 hours.

A brief example is below

	Rubrik	Nimble	Veeam	Tape	Rubrik	Nimble	Veeam
Site A	08:00	08:15	08:30	00:00	08:45	09:15	09:15
Site B	08:15	08:45	08:45	12:00	09:00	09:45	09:30
Site C	08:30		09:00		09:15		09:45

CHALLENGE 2

SINCE WHEN DID COMPUTER VIRUSES EAT BRAINS

SCENARIO 1:- NON CLOUD DATACENTERS

Sites

With this scenario we are assuming that the break out has occurred at our physical datacentres of which we control being the following

- Primary Site:- Mojave Desert (Back to Earth, 2016)
- Secondary Site:- NGD, Wales, United Kingdom

Recovery Plan

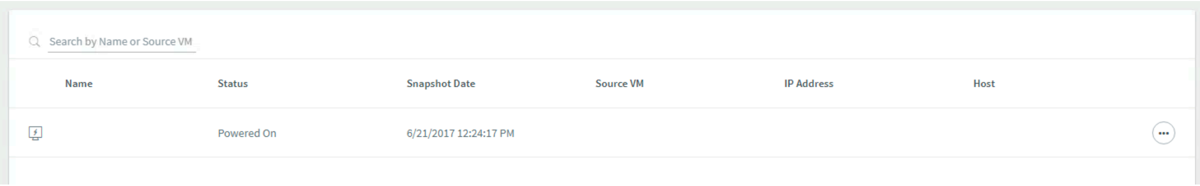
Our recovery plan will start by trying to isolate the machine running the crypto locker virus and shutting down the main SMB file servers. The Sophos engine should have alerted us into which machine was compromised and the Intercept X engine should have then shut down any network traffic.

File system recovery

We have multiple solutions to perform either a file recovery of which I can only assume this would be if Intercept X has functioned. If this solution had failed we could restore a snapshot from the Nimble storage array or live mount the Rubrik backup and storage VMotion this back to the Nimble array if we were happy that no further infection could occur. Both options offer a nice solution for testing to see if another attacked occurs as both restore methods are immutable and can be rolled back to the exact time again within minutes.

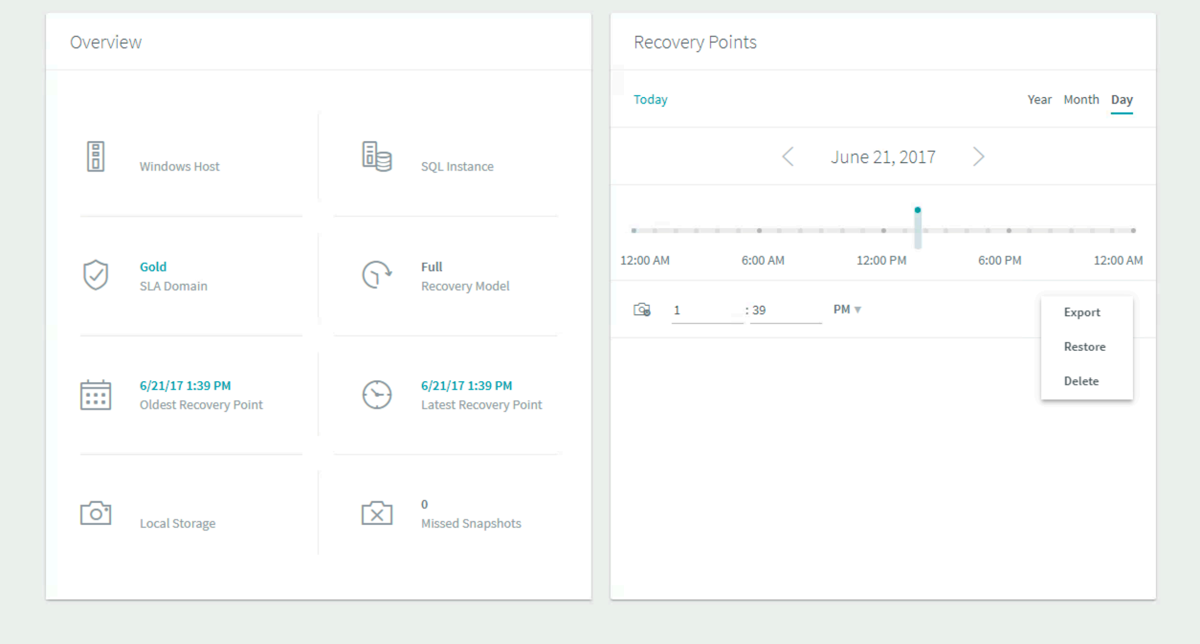
Rubrik Recovery

As mentioned above depending on the circumstances if this was merely only a few files that were overwritten or the database needed to be rolled back we could use the Rubrik restore options to do this. The first for file system recovery we would find the VM in the policies and click the 3 dots to either live mount this or use the analytics engine to search for a file within the VM. We could then either restore just the single file to the VM or download this locally to our machine for a manually restore. I have had to remove/simplify some of the screen shot to protect my lab environment



Name	Status	Snapshot Date	Source VM	IP Address	Host	
	Powered On	6/21/2017 12:24:17 PM				•••

The SQL backups are extremely powerful and allow down to the minute restoring if the SMB share of these are compromised for any reason. We can find the server and select an exact time for the system to restore the DB and then replay any of the logs.


Overview

Windows Host

SQL Instance

Gold
SLA Domain

Full
Recovery Model

6/21/17 1:39 PM
Oldest Recovery Point

6/21/17 1:39 PM
Latest Recovery Point

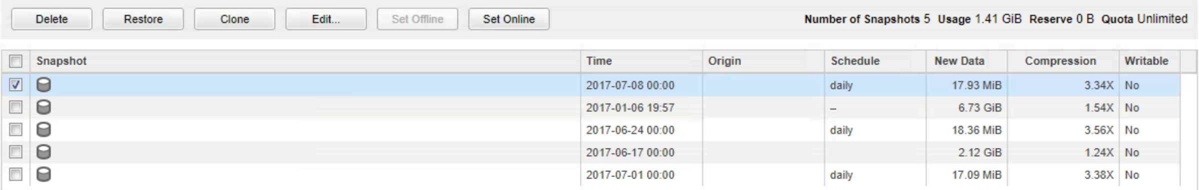
Local Storage

0
Missed Snapshots

Recovery Points

Core Storage Recovery

With the Nimble if the files cannot be recovered we can perform a full restore of the VM as per below.



Number of Snapshots 5 **Usage** 1.41 GiB **Reserve** 0 B **Quota** Unlimited

□	Snapshot	Time	Origin	Schedule	New Data	Compression	Writable
☑		2017-07-08 00:00		daily	17.93 MiB	3.34X	No
□		2017-01-06 19:57		–	6.73 GiB	1.54X	No
□		2017-06-24 00:00		daily	18.36 MiB	3.56X	No
□		2017-06-17 00:00			2.12 GiB	1.24X	No
□		2017-07-01 00:00		daily	17.09 MiB	3.38X	No

- Clone – The clone button allows us to do a zero copy clone consuming no more storage and allowing a boot or just the single volume as a separate drive
- Restore – Restore the running snapshot into production
- Set Online – Overwrites the current running version with this snapshot

Networking / WAN Recovery

Luckily for us we had a full list of MAC addresses of our switches in our CMDB. We are assuming the EatBrains virus is using an (ARP Spoofing) to try and simulate our routers and steal our traffic. For all our Windows systems we can run a PowerShell script like below to try and find rouge MAC addresses.

Firstly we need to enable remote management for PowerShel via GPOI and lock this down to our management machines.

Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service

Seek ARP Script

```
$RemoteComputers = Get-ADComputer -Filter * | select-object -expandproperty name



ForEach ($Computer in $RemoteComputers)

{

    Try

       {

          echo $Computer >> arplist.txt

           Invoke-Command -ComputerName $Computer -ScriptBlock {arp –a} >> arplist.txt  –ErrorAction Stop

       }

    Catch

       {

           Add-Content Unavailable-Computers.txt $Computer

       }

}
```

Once this script has run we can cross reference this with our CMDB and then try to find the rouge MAC address. From here we can look at the switching to see where this MAC is located and then try and connect to its IP. As the majority of our switches use SSH based keys we would be prompted that these have changed when we try to connect to the device. Once we have confirmed this and located the path on the other switches we can then isolate the rouge device. For example on the HP switches we could issue the command sh arp and on the Cisco we could hunt this down with a show mac address-table interface XX and then show ip arp vlan XYZ | include MAC-Address. We can then either reboot, refirmware or shut down the relevant ports to isolate the spread.

Firewalls

We are hoping if the firewalls have performed their tasks with one of the main firewalls being a Meraki MX that has behaviourally analysis built in. Once the file has been launched the logs are sent to Meraki and a copy of the executable for them to run and analyse of which if the behaviour is deemed malicious this is then blocked as per this article (Threat Grid for MX). This should then prevent any further call home or remote execution ability. For complete safety would could even create a rouge DNS entry for this to point to a dummy internal IIS site.

SCENARIO 2:- CLOUD DATACENTER

Sites

This part of the article is specifically targeting the ways we can improve the cloud datacentres and where we may lose some of the control

Recovery Plan

Our original design did not have any backup for the VMware on AWS and this would mean the whole datacentre would need to be rebuilt from scratch and then any data reseeded

Networking

As all the networking is managed and controlled by 3rd parties we would not easily be able to diagnose this and it would be suggested that we shut down the ports on all site to site connections and VPN tunnels whilst Amazon and VMware investigate. If they are in this network this would at least help prevent the spread and access to our other sites.

SCENARIO 3:- AUGMENTED DESIGN

Cloud Sites

As above we know there was items missing from our cloud datacentres. If we had the ability to re do these parts we would include at least 3 Rubrik nodes on AWS and also within the VMware on AWS environment to allow backup, replication and recovery in these environments.

WHAT WOULD I HAVE DONE DIFFERENT

There are many things I would have done different in this design such as augmented my application stack more and written some example code. I would have also built our more on my physical response plan. Unfortunately real life occurs and a few personal commitments have over taken my last few days but I really wanted to try and convey some of my ideas. I was missing my RPO and RTO table to better explain backups and reasons for choices which was a massive shame for me. I still feel the use of cloud data centres would put us at risk here as if the switches, router etc become infected and we are reliant on our 3rd party for a fix.

WORKS CITED

clstokes. (2016, Aug 24). *Deploy a Complex Infrastructure in AWS*. Retrieved from Deploy a Complex Infrastructure in AWS: https://github.com/hashicorp/atlas-examples/tree/master/infrastructures/terraform/projects/01

Edwards, G. (2016, July 01). *Back to Earth.* Retrieved from GitHub: Mojave Desert

GitHub. (n.d.). *GitHub HA*. Retrieved from GitHub Enterprise: https://help.github.com/enterprise/2.10/admin/guides/installation/high-availability-configuration/

Google, S. M. (n.d.). *Scribble Maps & Google.* Retrieved from Scribble Maps & Google: https://www.scribblemaps.com/maps/view/Mojave_Desert_/VDM_S5_EP1_GE

https://pixabay.com/en/users/geralt-9301/, g. (n.d.). *Pixabay*. Retrieved from Pixabay: https://pixabay.com/en/laptop-keyboard-cyber-attack-2450220/

https://pixabay.com/en/users/Mediamodifier-1567646/, M. (n.d.). *Broken Monitor on Risks Page*. Retrieved from Pixabay: https://pixabay.com/en/broken-business-monitor-2237920/

Meraki. (n.d.). *Threat Grid for MX*. Retrieved from https://meraki.cisco.com/blog/2017/06/introducing-threat-grid-for-meraki-mx/

Terraform. (n.d.). *Terraform*. Retrieved from https://www.terraform.io/#create: https://www.terraform.io/#create

CHALLENGE 2

SINCE WHEN DID COMPUTER VIRUSES EAT BRAINS

DISCLAIMER

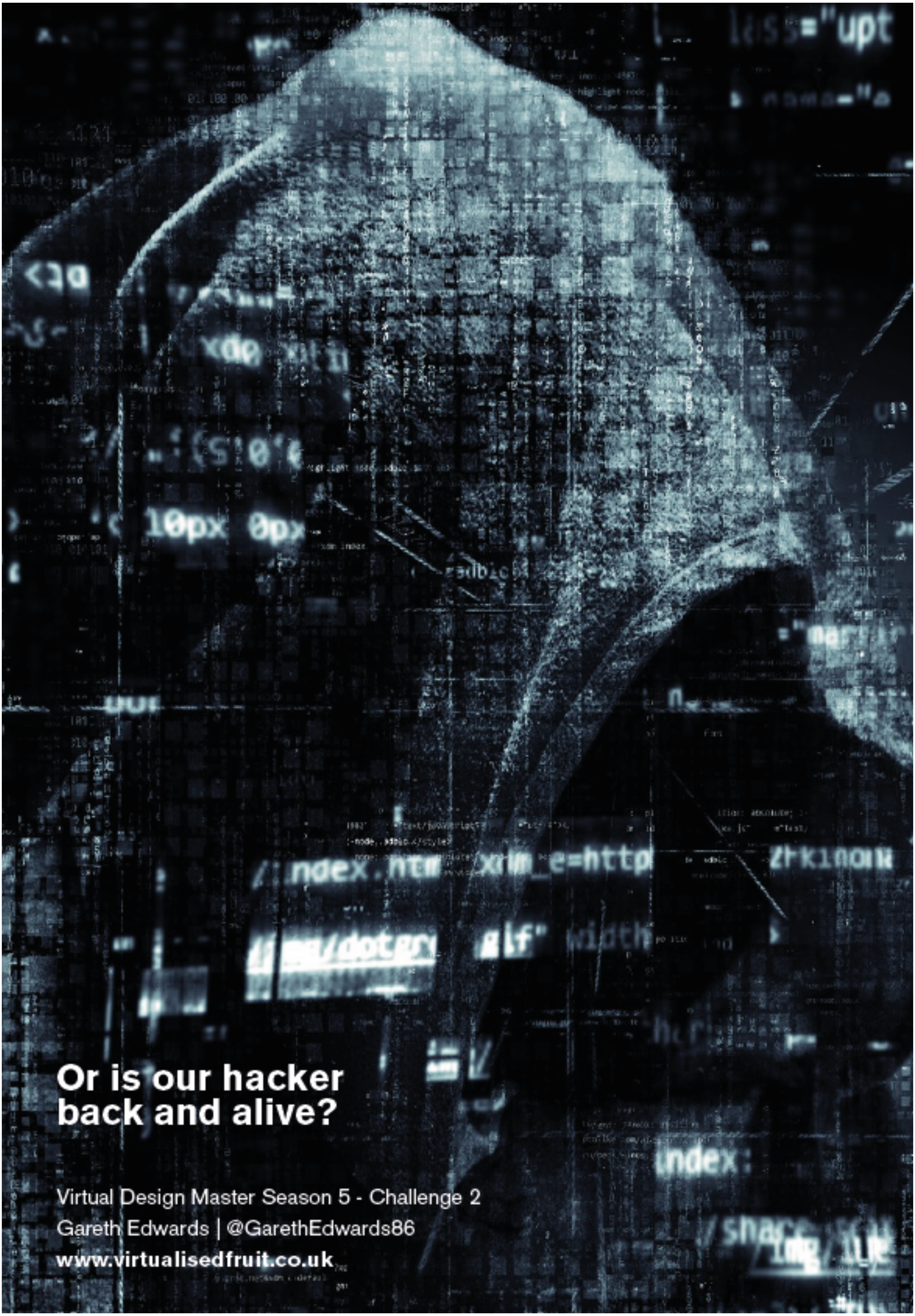
The view expressed in this document are my own and do not necessarily reflect the views of my current, previous or future employer(s). This is a fictional design and some elements may not work correctly within your infrastructure. All data and information provided on this document is for informational 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.

Covers were taken from the following places:-

https://pixabay.com/en/ransomware-cyber-crime-malware-2321110/

https://pixabay.com/en/hacker-cyber-crime-internet-2300772/

VERSION 1.0 JULY 2017



Or is our hacker back and alive?

Virtual Design Master Season 5 - Challenge 2

Gareth Edwards | @GarethEdwards86

www.virtualisedfruit.co.uk