Virtual Design Master

SEASON 5 – CHALLENGE 2

Dale Handley
@DALEMHANDLEY

11/07/2017

Table of Contents

1 Executive Summary

1.1 Mission objective

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.

1.2 Requirements

	Description
RE01	Secure the Infrastructure against the EatBrains virus
RE02	Find any and all compromised systems
RE03	Document a recovery plan for each layer of the infrastructure
RE04	Document a recovery plan for the HumanityLink 2.0 application
RE05	Include anything else that may thwart the Eatbrains virus

1.3 Constraints

	Description
C01	The design from Challenge 1 must be used

1.4 Assumptions

	Description
A01	Backups have not been encrypted by the Eatbrains ransomware
A02	The Eatbrains virus has not been sat dormant in our infrastructure for a period of time before starting to replicate itself and compromise other systems

1.5 Risks

	Description	Risk Mitigation
RI01	The Eatbrains virus could spread to our other Datacenters	Datacenter 1 should be taken offline immediately
RI02	Switches could be reinfected during execution of the recovery plan	Network devices will be disconnected from the network until they have all been remediated
RI03	Servers could be reinfected during execution of the recovery plan	NSX micro-segmentation will prevent unnecessary SMB communication between VMs

2 Securing the Infrastructure

2.1 Preventing further spread of the EatBrains virus

2.1.1 Isolate Datacenter 1

Datacenter 1 should be isolated from Datacenters 2 and 3 by physically removing the network uplinks. This will reduce our capacity to Terraform the Earth by 33% while we execute the recovery plan but it is the safest way to ensure that the virus does not replicate further and totally compromise our mission.

2.1.2 Implement NSX Micro-segmentation

Whilst NSX Micro-segmentation was part of the original design, failure to identify the correct Security Groups and Policies has allowed the EatBrains virus to run rampant through our network. Appropriate groups and policies have been identified in 'Appendix A: NSX Configuration'. NSX Micro-segmentation will ensure that VMs already infected will not be able to compromise any other system and also prevent reinfection during execution of the recovery plan.

2.2 Identify which devices have been compromised

To identify compromised devices two new products will be installed into the environment (vRealize Network Insight and AlienVault USM) and we will make use of one existing one (vRealize Operations Manager.)

2.2.1 vRealize Operations Manager

vRealize Operations Manager with Endpoint Operations has been monitoring the infrastructure since it was installed. Viewing the history of a Virtual Machine we can check for any anomalies such as spikes in CPU usage (a potential sign of files being encrypted) and new services being detected through Endpoint Operations.

2.2.2 vRealize Network Insight

vRealize Network Insight will be configured with three Data Sources:

- Netflow data from the ESXi hosts
- NSX Manager
- SSH account on the network devices

This will allow full visibility of the physical and virtual network, allowing easy identification of suspicious network traffic such as viruses trying to replicate themselves or a server trying to connect to a Command & Control server.

2.2.3 AlienVault Unified Security Management

The AlienVault USM all-in-one appliance will be deployed into Datacenter 1 (with remote sensors deployed into Datacenter 2 and 3.) AlienVault USM will be configured to use Netflow data from the ESXi hosts and will have a network interface connected to a SPAN port running in promiscuous mode. This software provides the following features:

- Asset Discovery – Active and Passive network scanning techniques will be used to identify the assets that are deployed in our network
- Vulnerability Assessment – Continuous vulnerability scanning of our infrastructure with remediation guidance
- Intrusion Detection – Network & Host-based IDS. File Integrity Monitoring will alert us to the presence of Ransomware viruses
- Behavioural Monitoring – Provides the ability to detect compromised systems through Netflow analysis and Full Packet Inspection
- Security Information & Event Management (SIEM) – AlienVault USM will be fed data from vRealize Log Insight and will provide Event Correlation and administrator alerts

3 Recovery Plan

3.1 Network Devices

All network devices should be physically isolated from each other (to prevent reinfection) and have their firmware re-flashed and configured from a known-good backup. We cannot begin to recover our infrastructure until we're confident that any network devices are free of viruses and not manipulating network traffic.

3.2 VMware Appliances (vRLI, vROPS)

vRealize Operations Manager and vRealize Log Insight are hardened Linux appliances using applicable guidelines of the UNIX SRG STIG. The appliances do not run any Samba services and as such are not vulnerable to the Eatbrains virus.

3.3 NTP Servers

The Samba service in CentOS 7 is not enabled by default, the server is protected by iptables and SELinux. The NTP servers show no signs of having been compromised.

3.4 Domain Controllers

To remove any traces of the Ransomware from the two Domain Controllers at Datacenter 1 the servers will need to be deleted from Active Directory and their metadata cleaned up. The DCs can then be rebuilt and promoted without fear of replicating the virus to Datacenter 2 and 3.

3.5 Veeam Backup & Recovery

To recover the Veeam server, the original server should be shut down and a replacement one built. The VMDK holding the data drive from the original server is attached to the new server. The Veeam software is then installed and a Configuration Backup is performed to import the existing backups onto the new server.

3.6 Recovering the HumanityLink 2.0 application

3.6.1 Recovering the Web and App tiers

The web and application tiers of the HumanityLink 2.0 application were built using Docker compose files. Using VMware Admiral the existing Containers are deleted and new ones deployed.

3.6.2 Recovering the Database tier

The HumanityLink application has been compromised and the integrity of the data in the Microsoft SQL database has been called into question. Using data taken from vROPS we believe that the Eatbrains virus outbreak luckily started sometime after the last successful backup of the SQL database based on a spike in CPU activity. We have no choice but to restore the database from the Veeam backup.

4 Appendix A: NSX Configuration

4.1 NSX Security Groups

The following NSX Security Groups will be configured

Name	Type	Description / Services provided
SG_ALLVMS	Dynamic	All VMs, excludes vCenter & NSX
SG_NTP	Static	NTP server
SG_ADDC	Static	DHCP, DNS, Active Directory
SG_VCSA	Static	vCenter server
SG_NSX	Static	NSX Manager and Controllers
SG_CONTAINER	Static	Harbor, Admiral, VIC
SG_VROPS	Static	vRealize Operations
SG_VRLI	Static	vRealize Log Insight
SG_VEEAM	Static	Veeam Backup and Replication
SG_HLWEB	Dynamic	HumanityLink 2.0 Web servers. Dynamic group based on partial VM name “HLWEB”
SG_HLAPP	Dynamic	HumanityLink 2.0 Application servers. Dynamic group based on partial VM name “HLAPP”
SG_HLDB	Static	HumanityLink 2.0 Database servers

4.2 NSX Services

Name	Description	Ports
SVC_MSSQL	Microsoft SQL Server	1433
SVC_SYSLOG	Syslog Communication	514, 1514
SVC_VRLIAGENT	vRLI Agent	9000, 9543

4.3 NSX Security Policies

Name	Source	Destination	Services	Action
SP_DEFAULT-BLOCK	SG_ALLVMS	SG_ALLVMS	ANY	Block
SP_TIME	ANY	SG_NTP	NTP	Allow
SP_DHCP	SG_HLWEB SG_HLAPP	SG_ADDC	DHCP	Allow
SP_DNS	ANY	SG_ADDC	DNS	Allow
SP_ADDS-AUTH	ANY	SG_ADDC	LDAP / LDAPS	Allow
SP_ADDS-REP	SG_ADDC	SG_ADDC	ANY	Allow
SP_CONTAINER	SG_CONTAINER	SG_VCSA	HTTPS	Allow
SP_VROPS-VCSA	SG_VROPS	SG_VCSA	HTTPS	Allow
SP_VROPS-EP	ANY	SG_VROPS	HTTPS	Allow
SP_VRLI	ANY	SG_VRLI	SVC_SYSLOG SVC_VRLIAGENT	Allow
SP_VEEAM	SG_VEEAM	SG_VCSA	HTTPS	Allow
SP_HLWEB	ANY	SG_HLWEB	HTTPS	Allow
SP_HLAPP	SG_HLWEB	SG_HLAPP	HTTPS	Allow
SP_HLDB	SG_HLAPP	SG_HLDB	SVC_MSSQL	Allow