Season 5

Challenge 2

EatBrains comes to town

Table of Contents

Status Report

We've been compromised with the EatBrains virus and ransomware, which is now rampant across our infrastructure. Here's what we know so far:

- The EatBrains Virus infects files and maps to SMB shares to spread further
- A variant that can store itself in memory on network devices and emulate routers
- Phone home features that allows for remote execution using infected devices in the environment

We have previously implemented security on a few different levels, which could help us mitigate some of the infection:

- RBAC credentials for management
- CHAP whenever possible for iSCSI targets
- SSH2/AES wherever possible
- Plaintext communications (telnet) access disabled

These considerations *should* help slow or prevent further spreading, however further analysis needs to be done.

We don't know yet how it got here, and we're not sure what the overall goal is, but we've got to find it, stop it, and make some changes so that it can't happen again.

Here's what we've deduced:

Requirements

R01	Define how to secure the infrastructure: Network, Compute, Infrastructure
R02	Determine how to find where the intruder breached and has remote execution capability
R03	Create a recovery plan for every layer of the network
R04	Create walk-through of how to recover compromised HumanityLink application system

Constraints

C01	The infection can emulate routers in network devices
C02	Phone-home features allows remote execution/command-and-control
C03	Original infection method is unknown
C04	Backups are only stored at remote sites

Assumptions

A01	Antivirus has already been deployed in the environment, and is functioning
A02	We can drop metrics/operations learning data between sites without issue
A03	We still have access to servers and equipment

A04	At least one machine and network device have been compromised
A05	A valid backup copy of firmware is available at each site (SHA1/MD5sum verified)
A06	The new variant is high-priority with antivirus vendors, and detection is imminent
A07	Drone ships are still functional and can ship data between sites (of course, navigating around impending weather if necessary)
A08	Sites are still capable of operating independently
A09	RPO of 1 hour was defined, however no RTO was defined

Risks

RI01	Original attack vector is unknown
RI02	Removal from systems (computers) requires successful detection by antivirus product (Trend Micro)
RI03	Offsite backups for each site are located 7 or 11 days away

Analyzing the situation

Initial Analysis

Through some slower, manual analysis of end-user symptoms where odd behavior and localized ransomware messages were obvious, we were able to determine ~~Larry~~ ~~Jerry~~ Garry Gergich in accounting clicked on a malicious link in an email, downloaded an attachment, ran as administrator, and infected his machine.

Given Garry's permissions on his mapped SMB shares and our previous implementation of RBAC, and the isolated nature of our three environments, the infection only appeared to spread between the 3 accounting users in Seattle, as well as the Seattle instance of the HumanityLink application system. It is still unknown, however, what networking equipment may be infected, or overall impact of the infection, other than being ransomwared.

To prevent further infections, we must first disconnect the sites from each other, as well as clean any/all sites, before reconnecting them together. This will not be disruptive to each site's operation overall, as they function independently [**A02**].

To improve our insight into the current state of affairs, but also to help detect a situation like this in the future, we need to implement a log analysis solution at each site to give administrators at each site the ability to search through events on a much quicker time scale. This will allow us to correlate events between infrastructure, network, and the virtualized infrastructure, to develop a holistic vision of events that are logged.

The first change we will make is to implement VMware's vRealize Log Insight for collection of logging events. This will be used to monitor all stacks in our deployment: Hardware and infrastructure (Cisco UCS, OpenStack), operating systems instances (Windows, Linux), and network devices (routers, switches).

Decision 1	Sever network connectivity between each site to prevent further spreading via network device
Decision 2	Manually review existing logs to determine point of infection
Decision 3	Implement vRealize Log Insight to speed up further analysis on Cisco UCS, OpenStack, Windows and Linux guests, and network equipment
Requirements Met	R01, R02
Justifications	We now have an independent point for log management for each site. we can get updated insight as to where we think the intruder breached, and where phone-home/command-and-control traffic is headed. Command-and-control traffic is not able to reach its destination, as we're removed each site from the internet, as well as each other, but we can see attempts.
Associated Risks	RI01: Log Insight node redundancy RI02: Log Insight cluster redundancy RI03: Log Insight cannot monitor itself
Risk Mitigation	RI01: Deploy Log Insight in a 3-node configuration RI02: Deploy an external log insight appliance to the site where backups are stored for that location (once connections are back) RI03: Forward collected logs to an external store

Threat Mitigation and Removal

It looks like Garry's special email was something previously unknown to our Trend Micro antivirus which is deployed on our server instances and end-user PCs. After immediately contacting Trend Micro and submitting a sample, they began working on analyzing, detection, and cleaning methods for its' antivirus products. Updated virus definitions have been obtained from the vendor via a sanitary 4G 'Hot Spot' from a mobile device, and uploaded into the existing infrastructure antivirus definition server. We must secure the existing infected PCs and prevent further propagation, secure our infrastructure against further attack, and restore any lost data from known good backups.

Decision 1	Update local virus and malware definitions from a sanitary connection
Decision 2	Scan, remove, and inoculate all computers/servers with the updated definitions
Decision 3	Wipe and reload existing networking equipment prior to re-establishing connections
Decision 4	Restore last-known configuration prior to infection on the Cisco UCS environment
Requirements Met	R03
Justifications	We must be able to clean every layer of our infrastructure from the infection. First, prevent it from spreading. Second, to remove the infections, and inoculate against further infections by updating the antivirus with the correct definitions
Associated Risks	RI01: Unknown infection methods and zero day vulnerabilities are unknown
Risk Mitigation	RI01: Establish RPO, RTO, and have a validated recovery plan

Recovery Operations

Existing Overview

Existing Infrastructure Backups:

- Cisco UCS Configuration
- Cisco router and switch configuration (auto-archive via SFTP)
- OpenStack infrastructure including instances and volumes

A meeting with application stakeholders determined a previously established RPO of 1 hour is acceptable, but in the event of a site being disconnected, and a recovery needed, 7 to 11 extra days for RTO is not acceptable (see Travel Time Table).

Additional Requirement

R05	**Establish 1-hour RPO, 8-hour RTO – defined 'Backups / Existing Overview'**

Travel Time Table (Transferring Remote Data via Automated Drone Ships)

Source	Destination	Travel Time (24kts)
Sydney, Australia	Tokyo, Japan	7 days
Tokyo, Japan	Seattle, WA	7 days
Seattle, WA	Sydney, Australia	11 days

Recovery Plan

In the event of a failure, compromise, or some other disaster, we must have a documented method and walkthrough of restoring configurations and data of the infrastructure, networking, instances, and data from the environment [**R03, R04**].

This recovery plan is identical to each site, and addresses the as-built data recovery methods assuming network connections are available to each site, or local copies are available. Order of operations is important to prevent further infection by network device once machines are inoculated.

All passwords throughout the organization will be required to change, enforcing password complexity, and a documented password policy.

Assumption

A01	Infected machines are clean and have been inoculated against further infection
A02	We still have access to the latest Cisco Gold Star firmware images and backups
A03	The latest firmware for network equipment inoculates it against the vulnerability that allowed EatBrains to infect and run in-memory

Requirements

R03	Create a recovery plan for every layer of the network
R04	Create walk-through of how to recover compromised HumanityLink application system

Networking

Local images for routers and switches are retained in a (non SMB) repository of the latest gold-star Cisco device images, with both SHA1 and MD5sums for verification:

- Firmware images can be validated prior to installation
- Configurations can be re-imported from a local repository

Infrastructure

Cisco UCS Backup and Restore

Full State backups with encryption are taken daily, and saved to a local repository, which is then backed up off-site utilizing Raksha.

In the event of a UCS configuration restore, the latest known-valid configuration can be restored.

Once the UCS configuration has been restored, we can move on to the OpenStack Infrastructure.

Instances and Data

To restore an instance from the Raksha repository (local or remote), the following pseudocode algorithm can be used:

```
for each resource in backupjobrun_vm_resources
    download all the components of a backup to a temporary location


for each resource in backupjobrun_vm_resources
    download all the components of a backup to a temporary location.
    rebase the qcow2 files to the correct backing files
        qemu-img  rebase –b  backing_file_base  backing_file_top
    commit and flatten the qcow2 files
        qemu-img commit  backing_file_top
    upload images and create volumes


for a boot device, if the image doesn’t exist in glance, upload the image to glance.


for a data volume, we need to upload the backup to glance as an image and covert that
to a cinder volume.
(TODO: See if Cinder can help us to create a block volume from a file instead of an i
mage).


use nova to create a new instance
```

HumanityLink Restoration

Unfortunately, Mr. Gergich’s magic email has managed to infect Seattle, Washingon’s instance of the HumanityLink application, and our HumanityLink data for this site has been scrambled.

Utilizing the above methods of first securing the rest of the environment, our recovery plan is to utilize our existing methods and Raksha volume snapshots and backups to restore all volumes, instances, and services associated with HumanityLink to a working point in time.

HumanityLink application engineers will validate datasets.

Our distributed method of having HumanityLink be unique and self-sufficient at each site prevented a much larger disaster, however there’s some things we can change for the future.

Backup Infrastructure Change

The second change we will implement following this successful recovery is to make sure each site also has a local backup of itself, as well as one copy at a remote site to meet RPO and RTO requirements.

Decision 1	Implement local backups, alongside remote backups
Requirements Met	R05
Justifications	We must meet 1 hour RPO and 8 hour RTO from both local and remote backups. If we do not have access to local snapshots or backups, data transfer time is 7 to 11 days.
Associated Constraint	RI01: Additional infrastructure (storage) will be required
Constraint Mitigation	RI01: Acquire required storage to facilitate local backups.

Additional Security Changes

- Access to network devices will be secured with strong passwords
- All unused ports on network devices will be disabled
- Firewall roles will be modified to only allow traffic on predefined ports externally
- L3 access lists implemented between sites for inter-site security
- Activity on network devices (switches, routers, firewall) will be monitored with configured alerts to appropriate security staff
- All employees will receive additional security training
- Operating systems (Windows, Linux) will be configured to vendor security hardening standards

Original Design Changes Notes

Log Collection

A log collection tool, vRealize log insight, has been deployed to each site

Backup Policy

An RPO and RTO have been defined, which must account for each site being disconnected or orphaned from its' offsite backups. With this, introduced requirement of acquiring additional backup space

Additional Backup Hardware

To meet local RPO and RTO, additional backup hardware has been acquired.

References

Cisco. (2017, June 02). *Cisco*. Retrieved July 11, 2017, from Cisco UCS Manager Administration Management Guide 3.1 : http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/GUI-User-Guides/Admin-Management/3-1/b_Cisco_UCS_Admin_Mgmt_Guide_3_1/b_Cisco_UCS_Admin_Mgmt_Guide_3_1_chapter_01001.html

Jr., T. R. (2016, February 12). *VMware Blogs*. Retrieved July 11, 2017, from VMware Integrated OpenStack Video Series: OpenStack Log Analysis with vRealize Log Insight : https://blogs.vmware.com/openstack/vmware-integrated-openstack-video-series-openstack-log-analysis-with-vrealize-log-insight/

OpenStack. (2017). *Raksha*. Retrieved from OpenStack Wiki: https://wiki.openstack.org/wiki/Raksha#Restore