Beyond ‘Check The Box’

Powering Intrusion Investigations

PRESENTED BY: Jim Aldridge

1 OCTOBER 2015

- Mapping an IP address to a hostname
- Identifying the systems to which a specified account authenticated
- Determining the systems that communicated with a specified Internet IP address
- Tracking domain name resolution attempts
- Identifying forensic artifacts across the environment

1. What information was exposed?

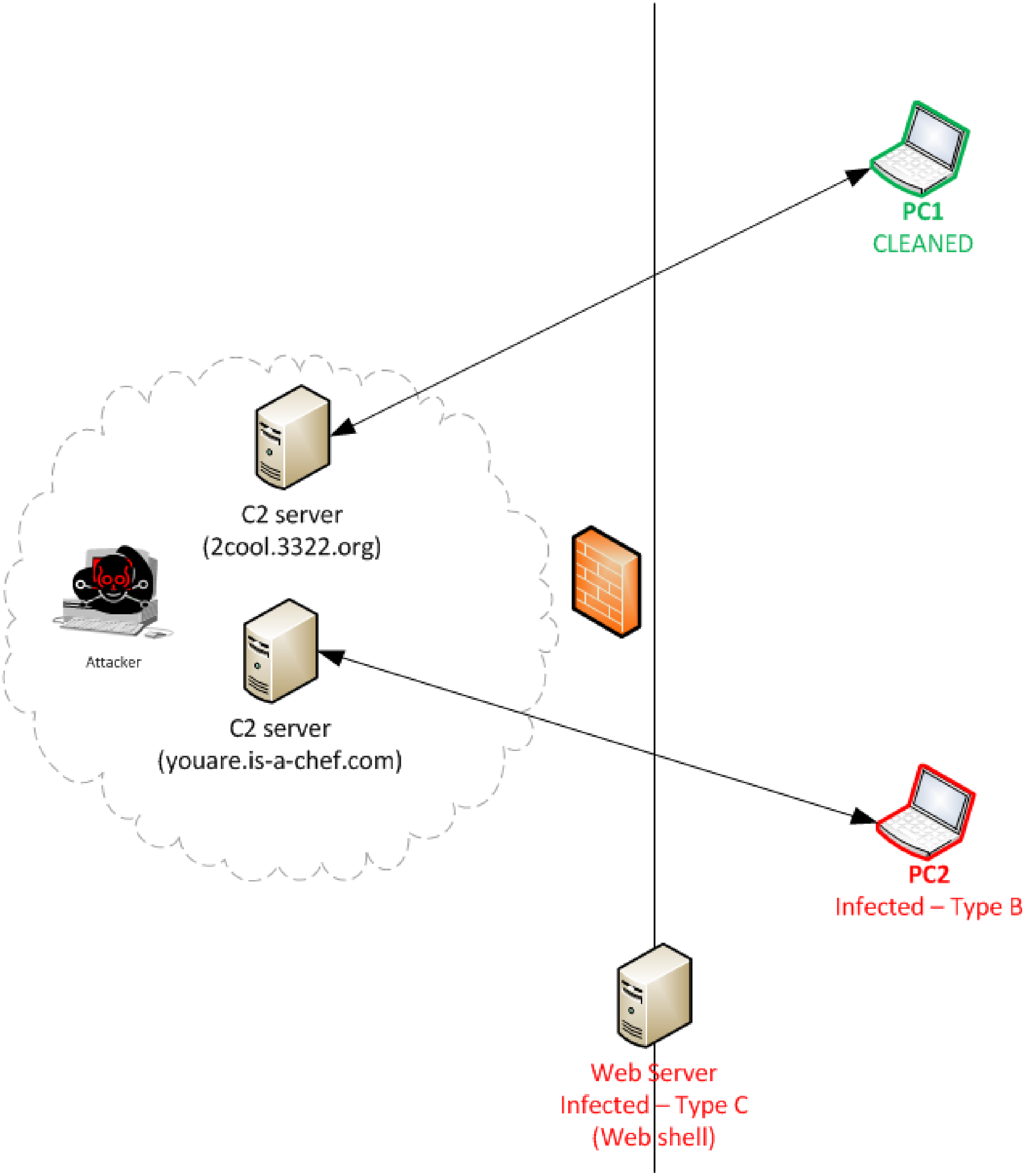
2. Do I need to notify regulators or customers?

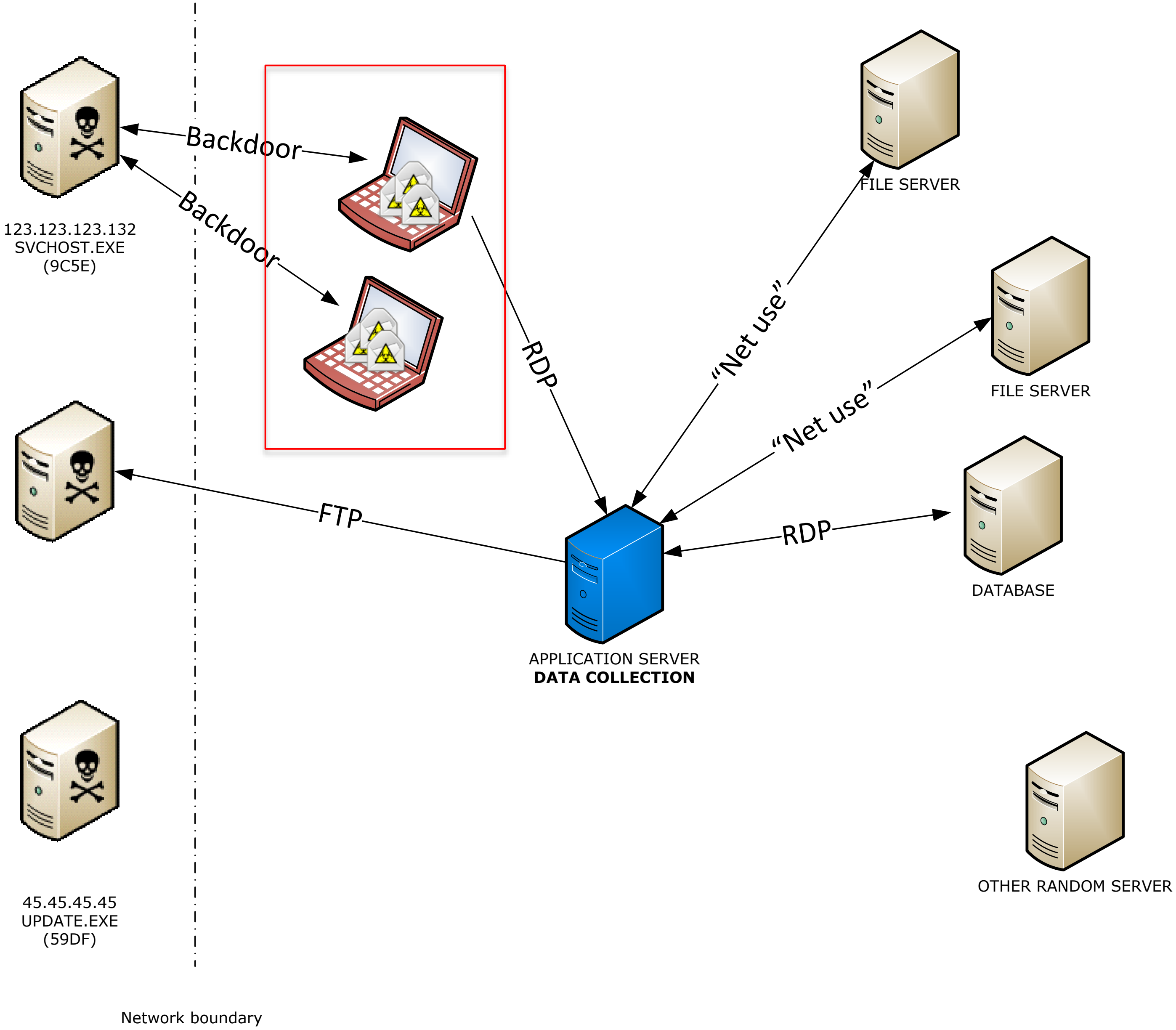
3. What is the extent of the compromise?

4. How much money did we lose?

5. How did the attacker gain entry?

6. How do we effectively stop the attack and remove the attacker?


PC1
CLEANED
C2 server
(2cool.3322.org)
Attacker
C2 server
(youare.is-a-chef.com)
PC2
Infected – Type B
Web Server
Infected – Type C
(Web shell)


123.123.123.132
SVCHOST.EXE
(9C5E)
Backdoor
Backdoor
RDP
"Net use"
"Net use"
FILE SERVER
FILE SERVER
DATABASE
FTP
RDP
APPLICATION SERVER
DATA COLLECTION
OTHER RANDOM SERVER
45.45.45.45
UPDATE.EXE
(59DF)
Network boundary

- When and what was the earliest evidence of compromise?
- How did the attacker gain entry?
- What is the latest evidence of attacker activity?
- What systems are (or were previously) under the attacker’s control?
- What systems did the attacker access?
- What actions did the attacker execute on the systems with which he interacted?
- How does the attacker maintain access to the environment?
- How does the attacker operate inside of the environment?
- What tools has the attacker deployed?
- What accounts did the attacker compromise?

#1: Mapping an IP address to a hostname

Event date: 7/22/13

Intruder C2 node IP: 123.123.123.132

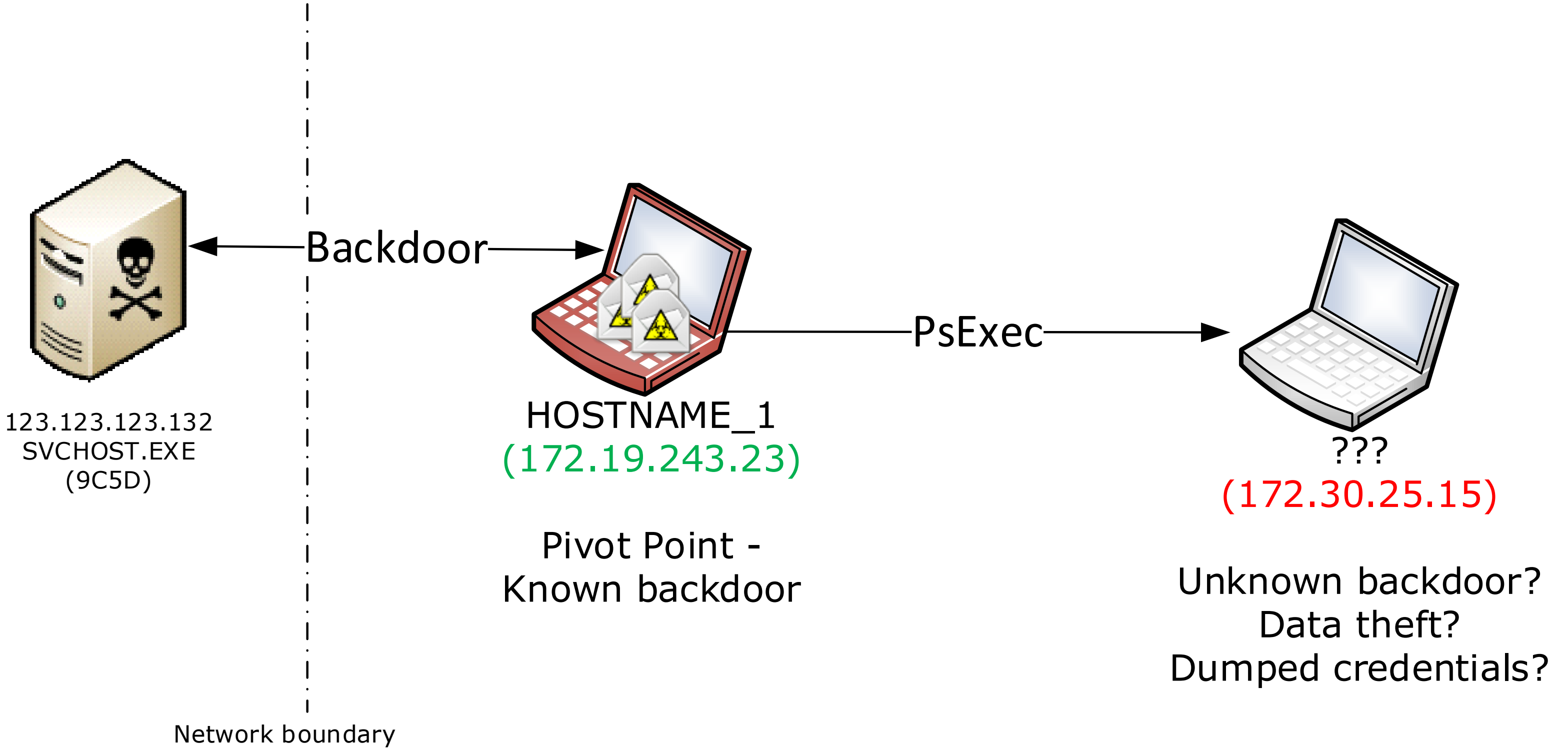
ORG Pivot Point IP: 172.19.243.23

ORG Pivot Point TCP Port Utilized: 23

Method of access: A previously installed remote access agent initiated communications with the intruder's C2 node listed above.

List of ORG systems accessed from the Pivot Point: SYSTEM1 (172.27.31.95), SYSTEM2 (192.168.2.55), **unknown (172.30.25.15)**

…



123.123.123.132
SVCHOST.EXE
(9C5D)

Backdoor

Network boundary

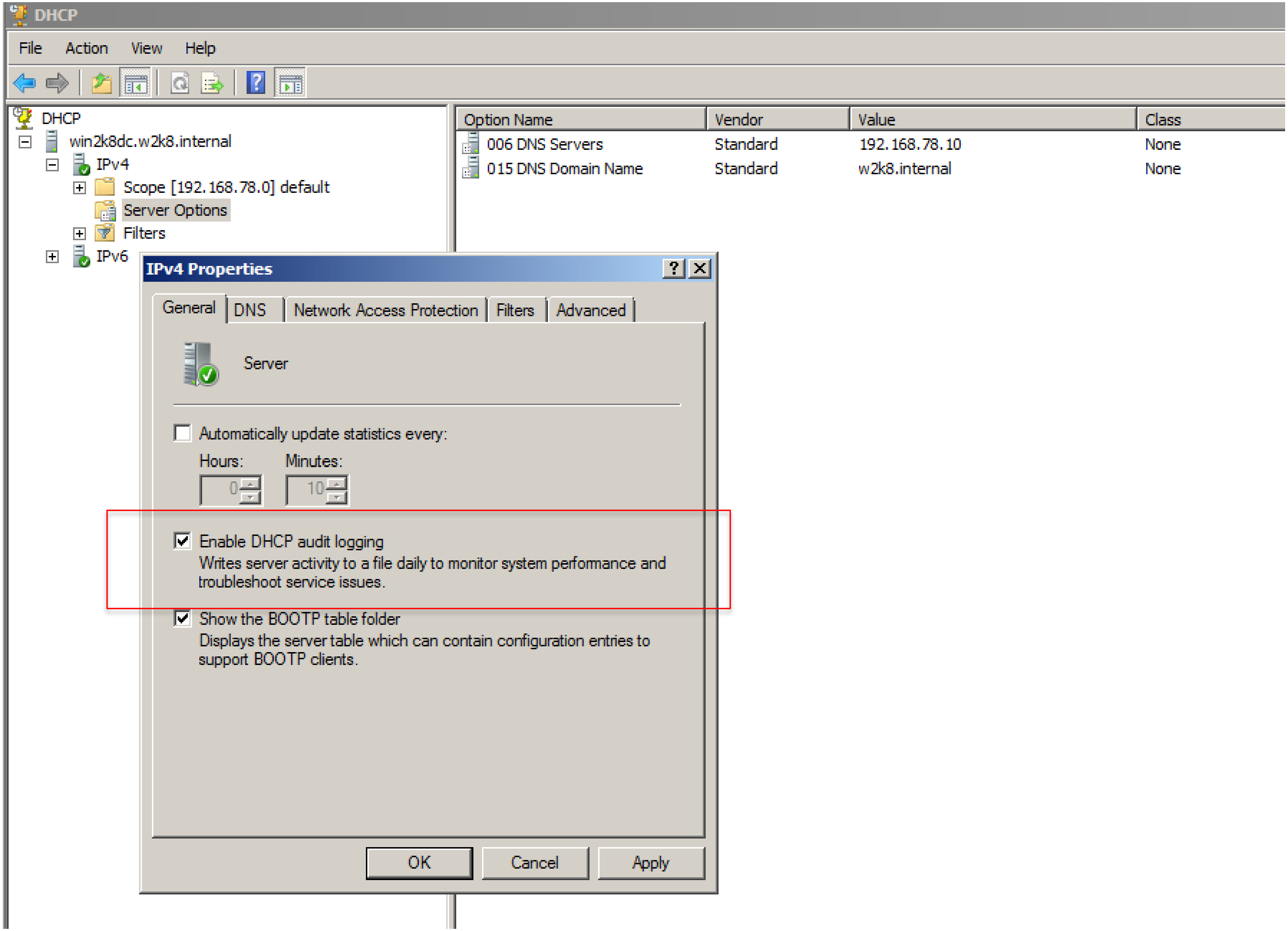
HOSTNAME_1
(172.19.243.23)

Pivot Point -
Known backdoor

PsExec

???
(172.30.25.15)

Unknown backdoor?
Data theft?
Dumped credentials?



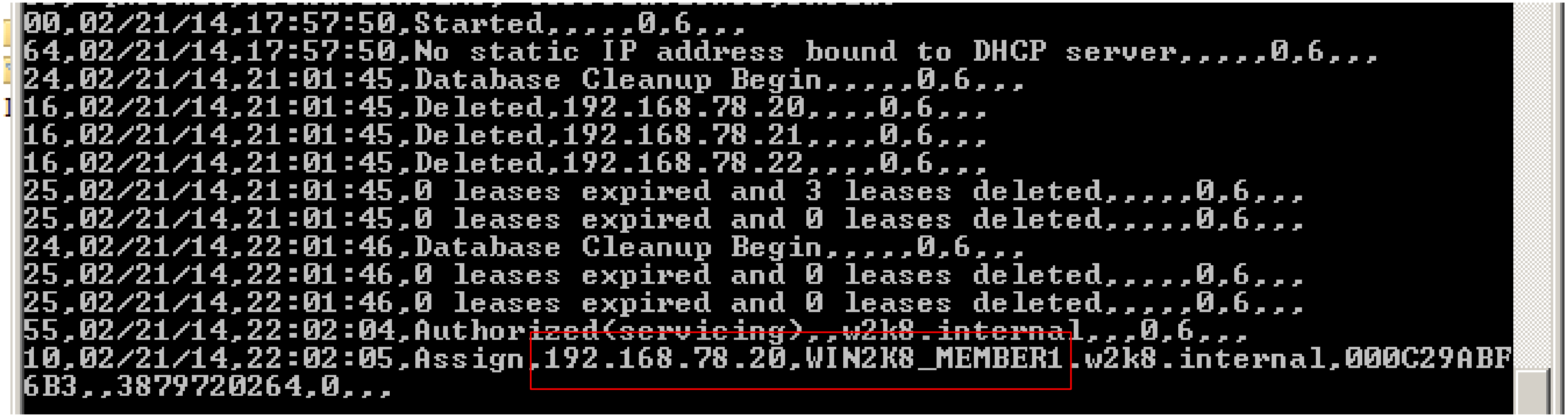
Option Name	Vendor	Value	Class
006 DNS Servers	Standard	192.168.78.10	None
015 DNS Domain Name	Standard	w2k8.internal	None

□ Automatically update statistics every:

Hours: 0 Minutes: 10

☑ Enable DHCP audit logging
Writes server activity to a file daily to monitor system performance and troubleshoot service issues.

☑ Show the BOOTP table folder
Displays the server table which can contain configuration entries to support BOOTP clients.

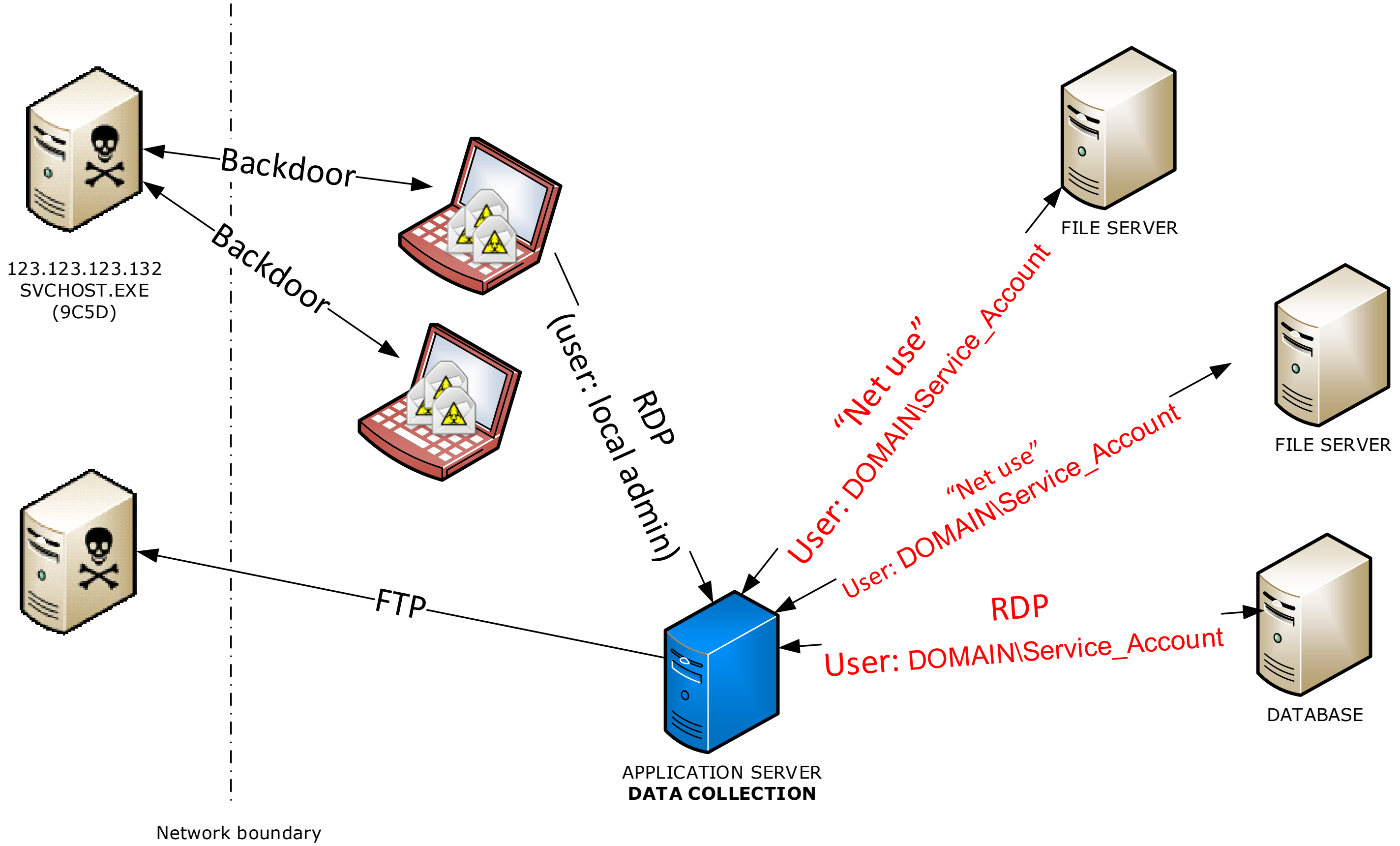


```
00,02/21/14,17:57:50,Started,,,,,0,6,,,
64,02/21/14,17:57:50,No static IP address bound to DHCP server,,,,,0,6,,,
24,02/21/14,21:01:45,Database Cleanup Begin,,,,,0,6,,,
16,02/21/14,21:01:45,Deleted,192.168.78.20,,,,0,6,,,
16,02/21/14,21:01:45,Deleted,192.168.78.21,,,,0,6,,,
16,02/21/14,21:01:45,Deleted,192.168.78.22,,,,0,6,,,
25,02/21/14,21:01:45,0 leases expired and 3 leases deleted,,,,,0,6,,,
25,02/21/14,21:01:45,0 leases expired and 0 leases deleted,,,,,0,6,,,
24,02/21/14,22:01:46,Database Cleanup Begin,,,,,0,6,,,
25,02/21/14,22:01:46,0 leases expired and 0 leases deleted,,,,,0,6,,,
25,02/21/14,22:01:46,0 leases expired and 0 leases deleted,,,,,0,6,,,
55,02/21/14,22:02:04,Authorized(servicing),,w2k8.internal,,,0,6,,,
10,02/21/14,22:02:05,Assign,192.168.78.20,WIN2K8_MEMBER1.w2k8.internal,000C29ABF
6B3,,3879720264,0,,,
```

#1: Mapping an IP address to a hostname

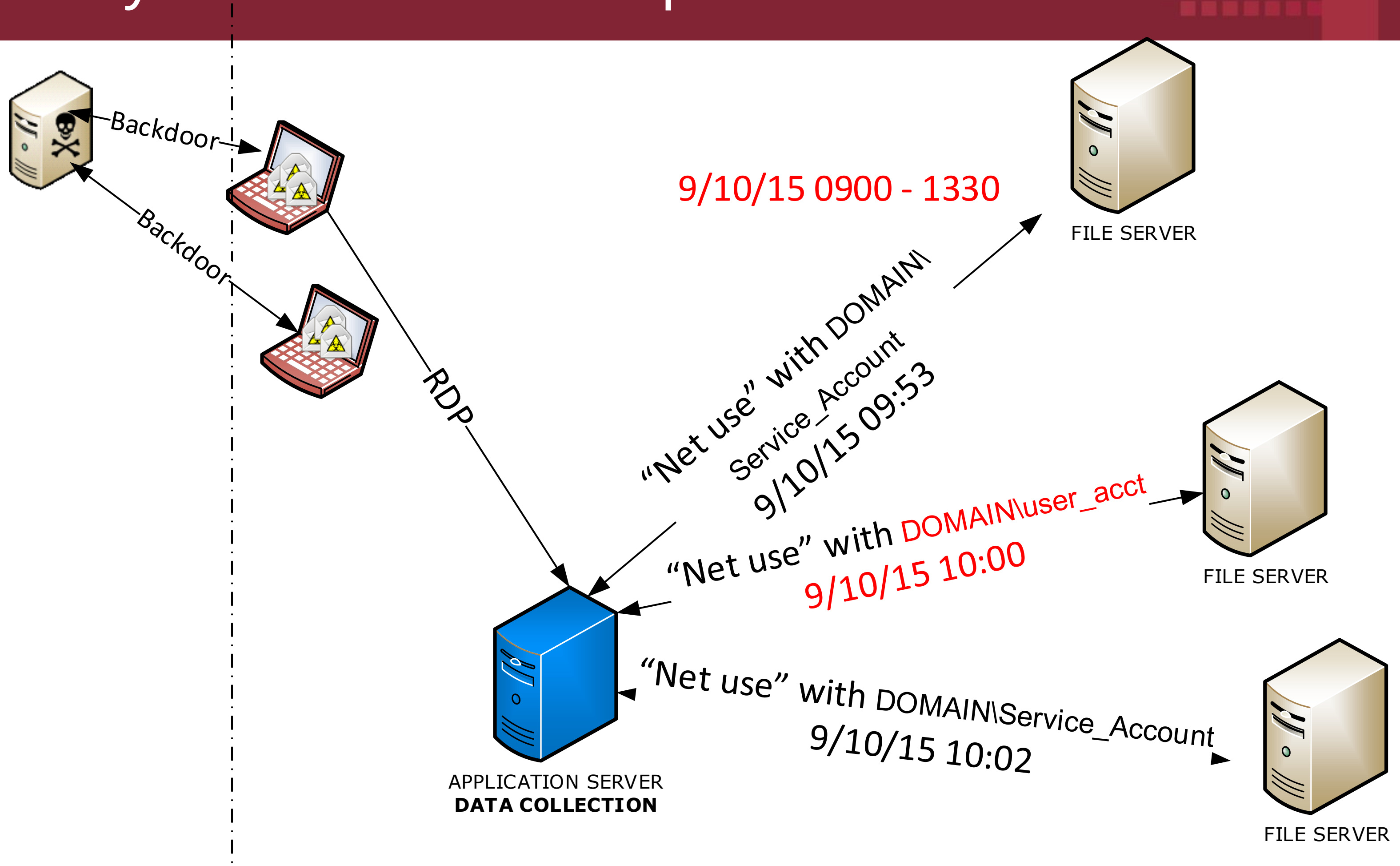
- Ensure the logs are enabled
  - DHCP audit logs are located by default at %windir%\System32\Dhcp (Win2k8)
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DHCPServer\Parameters\DhcpLogFilesMaxSize (max size in MB)
  - Reference: http://technet.microsoft.com/en-us/library/cc726869(v=ws.10).aspx
- Collect logs, make searchable, and archive
  - SIEM (ideal)
  - Scheduled task to copy log files off and compress to a central file share daily
    - PowerGREP is your friend

#2: Systems to which a specified account authenticated



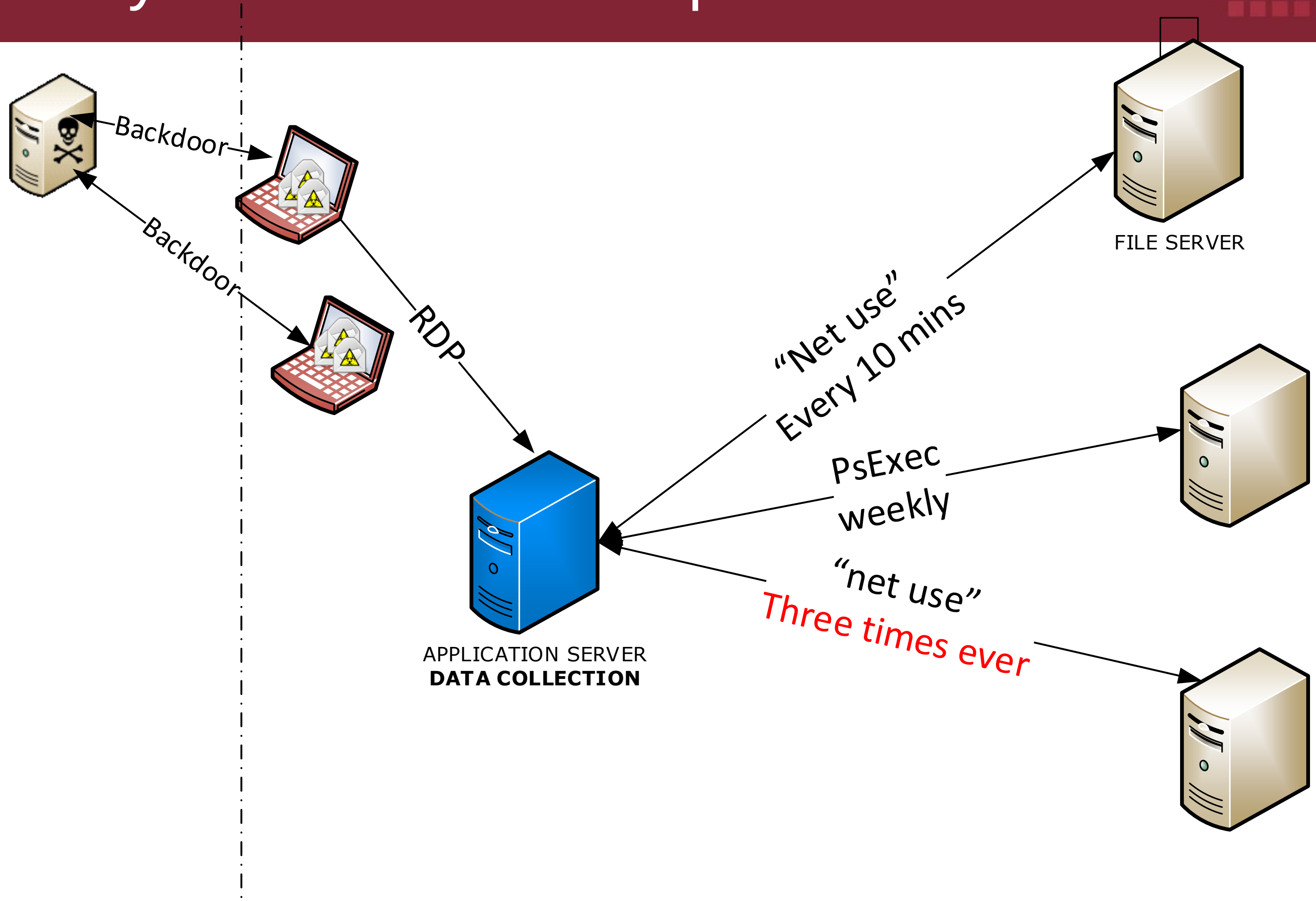
"DOMAIN\Service_Account": where did the account authenticate?

#2: Systems to which a specified account authenticated


Backdoor
Backdoor
RDP
9/10/15 0900 - 1330
FILE SERVER
"Net use" with DOMAIN\Service_Account 9/10/15 09:53
FILE SERVER
"Net use" with DOMAIN\user_acct 9/10/15 10:00
"Net use" with DOMAIN\Service_Account 9/10/15 10:02
FILE SERVER
APPLICATION SERVER
DATA COLLECTION

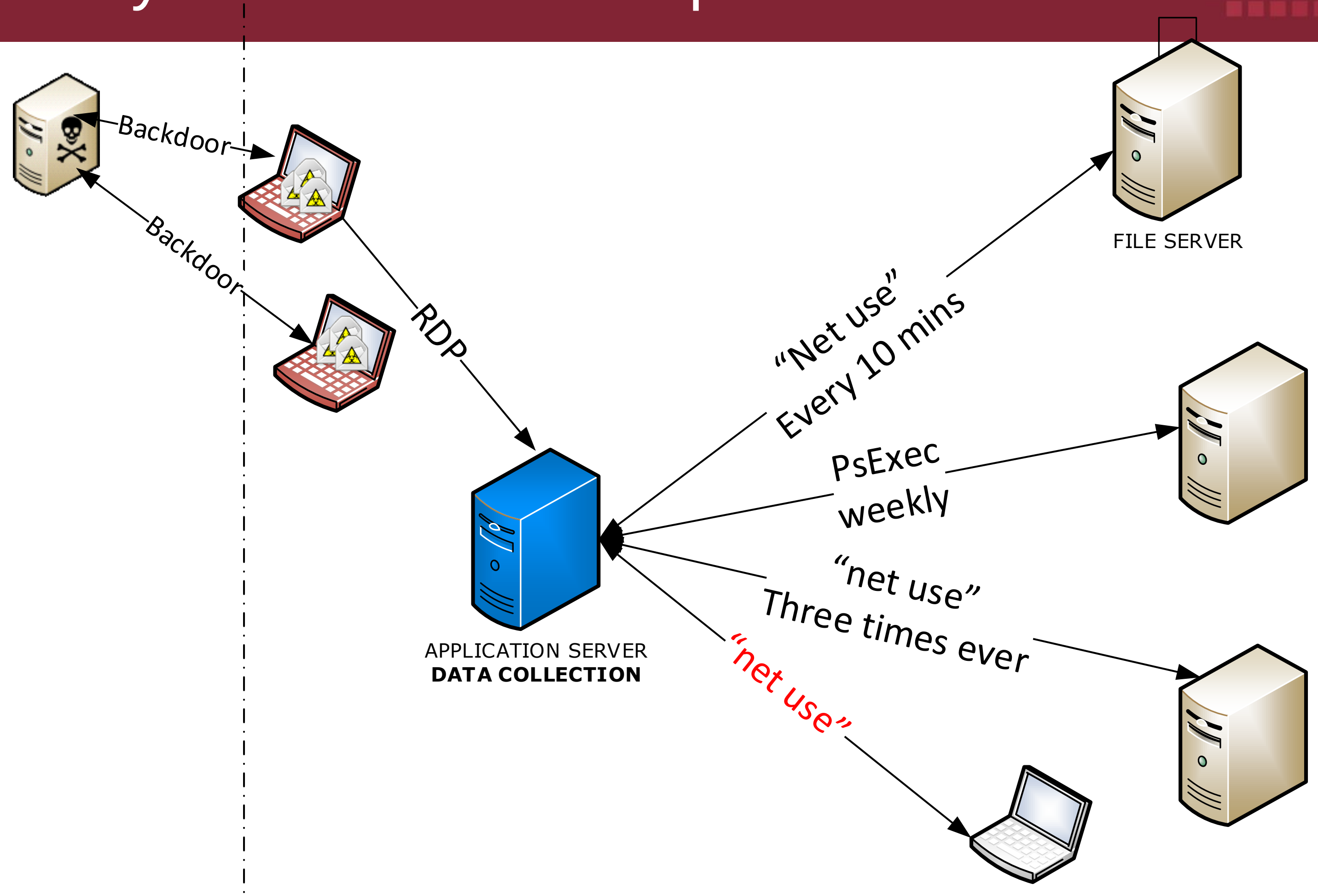
From the application server (known compromised), given time range: **to** which systems did any account connect to during that window?

#2: Systems to which a specified account authenticated



Looking across all servers, where do you see logins **from the application server?**

#2: Systems to which a specified account authenticated

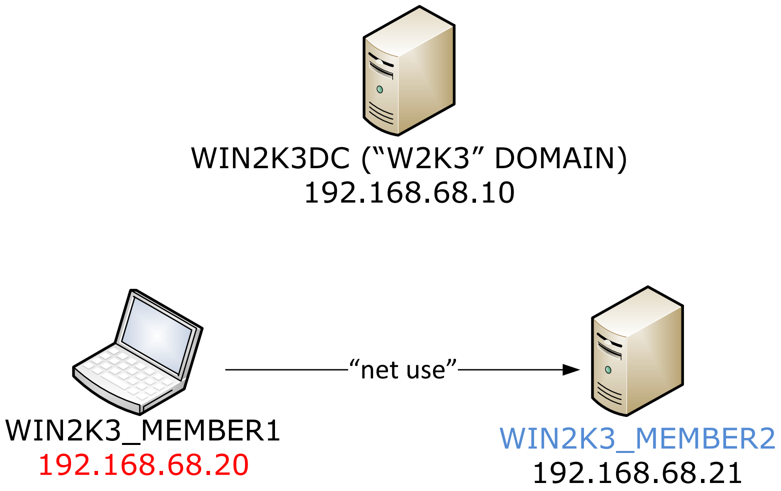


Looking across all ~~servers~~ systems, where do you see logins **from the application server?**

© Mandiant Corporation. All rights reserved.

```
Service Ticket Request:

User Name:                    user001@W2K3.LOCAL
User Domain:                    W2K3.LOCAL
Service Name:                    WIN2K3_MEMBER2$
Service ID:                     %{S-1-5-21-
363441063-1095074585-2989622239-1114}
Ticket Options:                     0x40810000
Ticket Encryption Type:             0x17
Client Address:                     192.168.68.20
Failure Code:                     -
Logon GUID:                     {e851c668-2ee0-1ee6-
04c8-f872b94da293}
Transited Services:             -
```



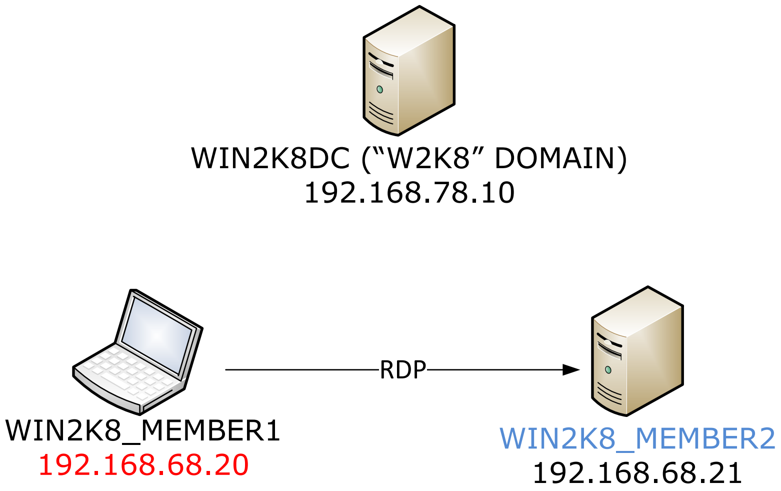
```
A Kerberos service ticket was requested.

Account Information:
Account Name:    user002@W2K8.INTERNAL
Account Domain:      W2K8.INTERNAL
Logon GUID:      {FE8E39B0-70D2-2A2F-21D5-
311EEFC11E1F}

Service Information:
Service Name:    WIN2K8_MEMBER2$
Service ID:      S-1-5-21-465013511-4273241566-
1457102820-1107
Network Information:
Client Address:      ::ffff:192.168.78.20
Client Port:     49204
```

RDP
Win 2008
With "NLA"

http://technet.microsoft.com/en-us/library/cc732713.aspx



WIN2K8DC ("W2K8" DOMAIN)
192.168.78.10

RDP

WIN2K8_MEMBER1
192.168.68.20

WIN2K8_MEMBER2
192.168.68.21

#2: Systems to which a specified account authenticated

- Log authentication events
  - On all systems!
  - Successful more important than failed
  - Very important, even if you do not have a way to search or aggregate them
- At a minimum, push domain controller logs into a SIEM
  - Or copy off logs to a central location for manual searching
  - This will enable querying Kerberos Service Tickets
  - Realize that you don’t have visibility into local account activity
    - Can make up for that “on the fly”, under Capability #5, but only if you have been logging for the data

Authentication-related Logging Recommendations

Audit	Setting	Scope	Important EIDs
Account Logon: Audit Credential Validation	Success Failure	All	4776 (Account validated)
Account Logon: Audit Kerberos Authentication Service	Success	Domain Controllers	4768 (Kerberos TGT requested)
Account Logon: Audit Kerberos Service Ticket Operations	Success	Domain Controllers	4769 (Kerberos service ticket requested)
Account Logon: Audit Other Account Logon Events	Success	All	4778 (session reconnected to window station)
Logon/Logoff: Audit Account Lockout	Success	All	4625 (account locked out)
Logon/Logoff: Audit Logoff	Success	All	4634, 4647 (account logged off)
Logon/Logoff: Audit Logon	Success / Failure	All	4624, 4648 (account logged on, explicit credentials logon)

*Windows 7/2008; reference: http://technet.microsoft.com/en-us/library/dd772662(v=ws.10).aspx
*Also reference Randy Franklin Smith's UltimateWindowsSecurity.com site for great descriptions of event IDs: http://www.ultimatewindowssecurity.com/Default.aspx

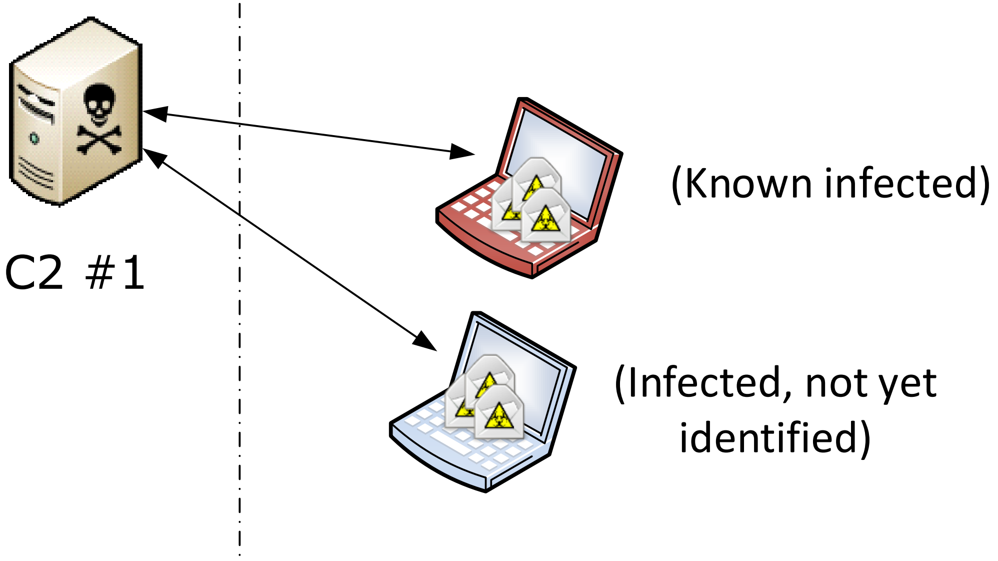
#3: Determining the systems that communicated with a specified Internet IP address

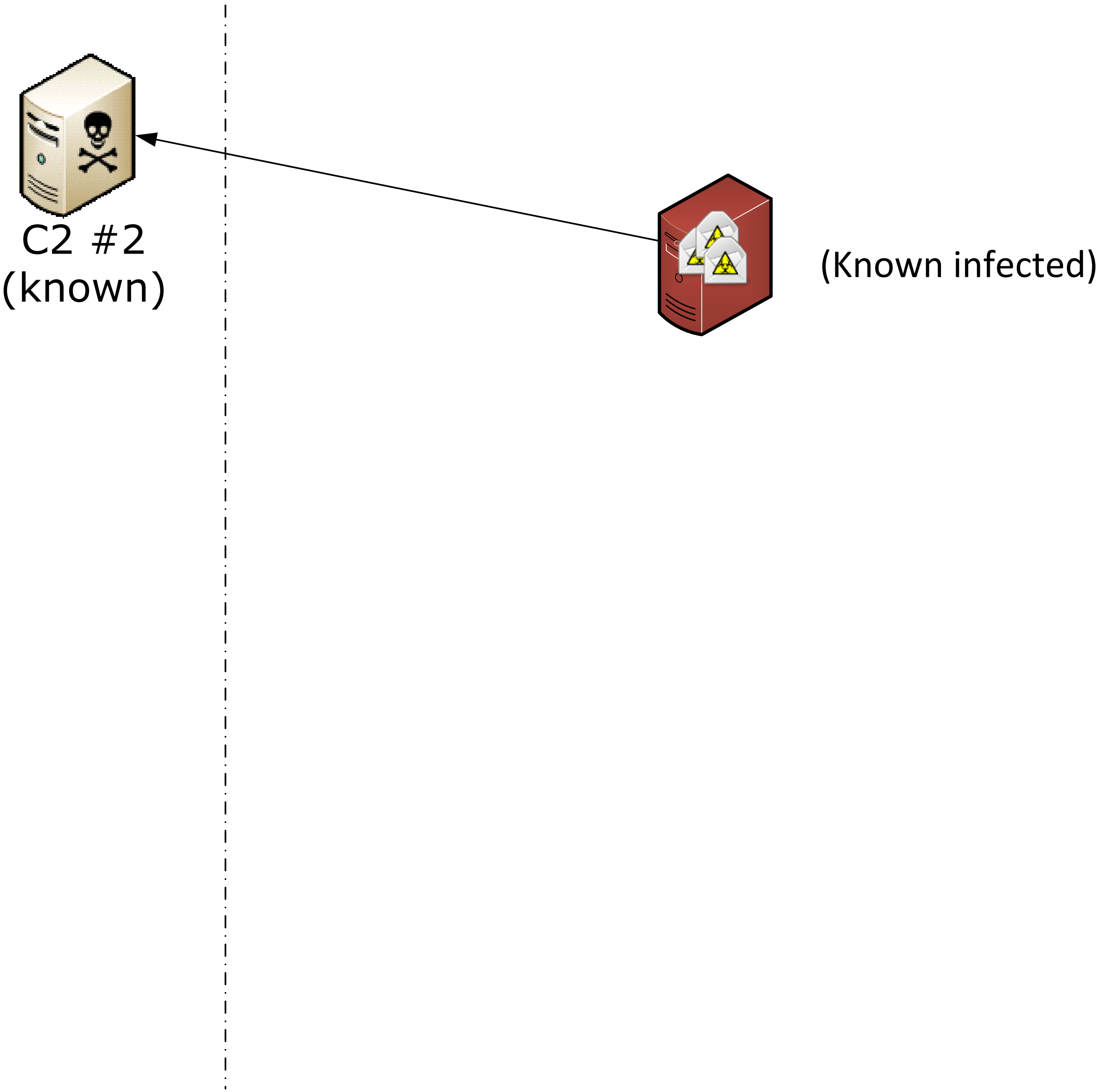
Event date: 7/22/13
Intruder C2 node IP: 123.45.67.8 **(C2 #1)**
ORG Pivot Point IP: 172.19.243.23
ORG Pivot Point TCP Port Utilized: 23

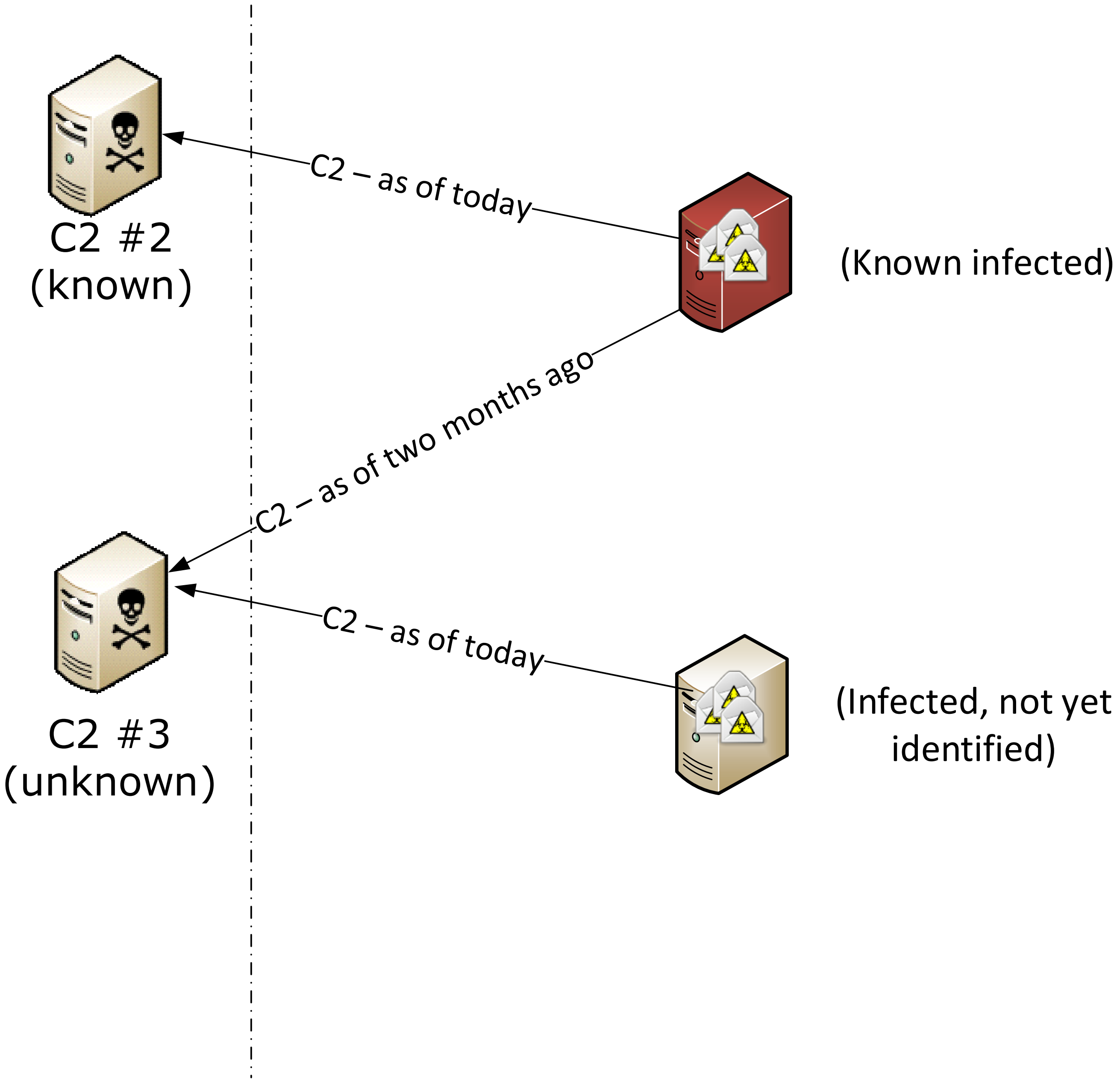
…

Other actions: Configured a previously installed backdoor on INFECTED2 to communicate with IP 23.45.67.89. **(C2 #2)**

The backdoor was previously configured to communicate with IP 34.56.78.91. **(C2 #3)**

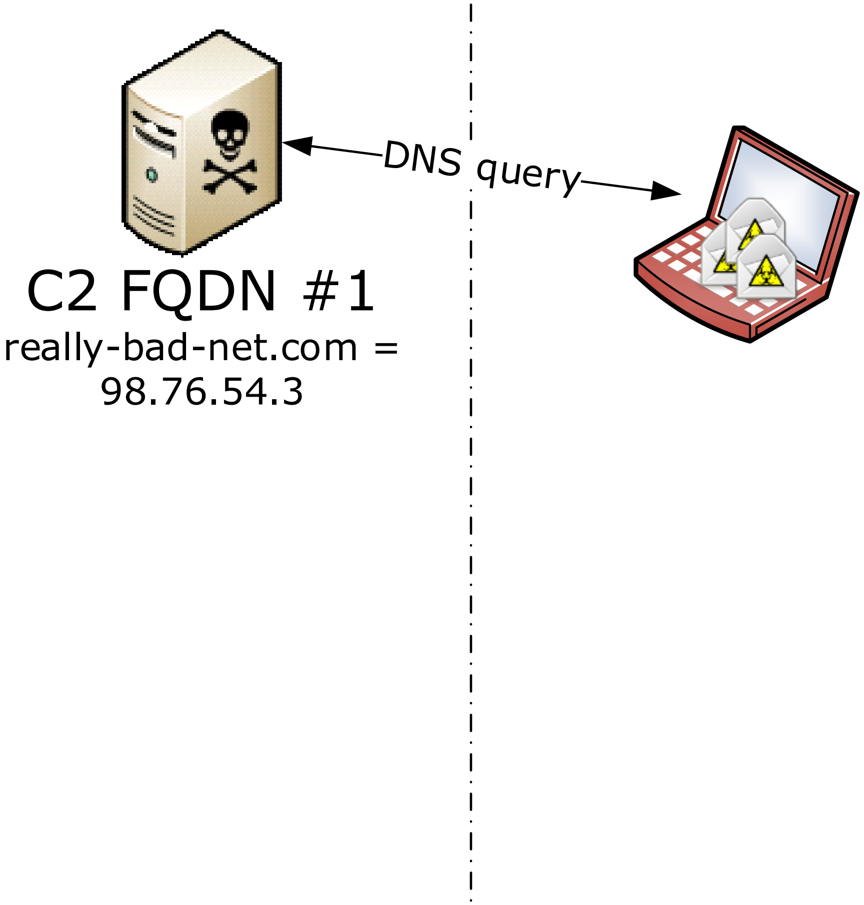

C2 #1
(Known infected)
(Infected, not yet identified)

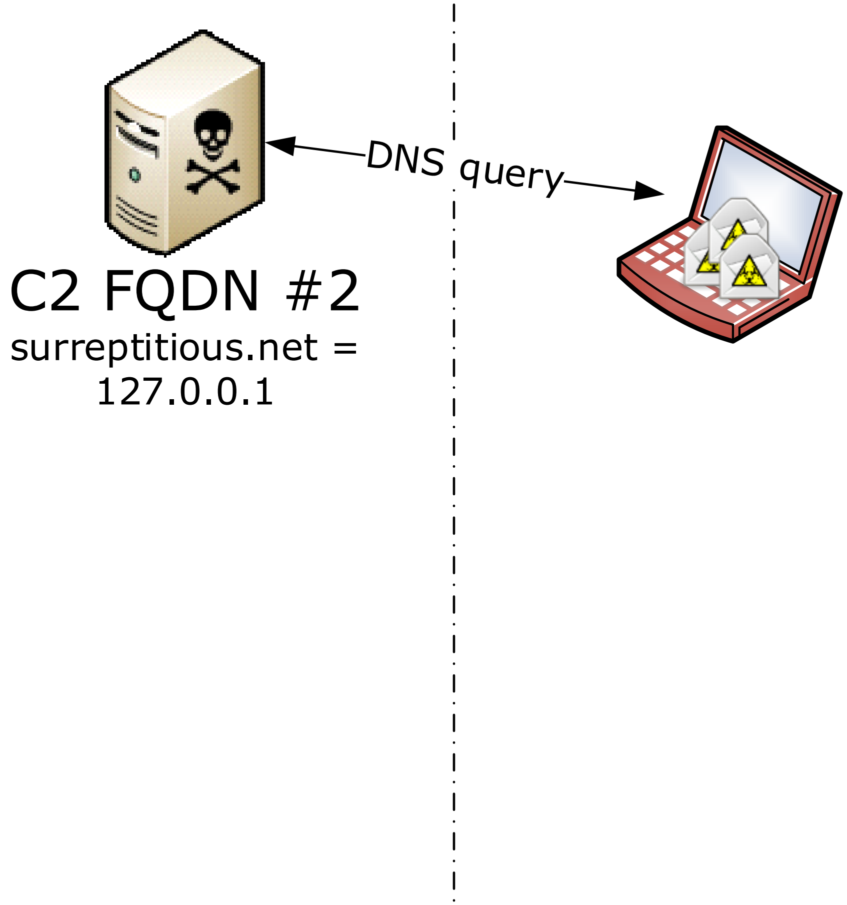

C2 #2
(known)
(Known infected)


C2 #2
(known)
C2 – as of today
(Known infected)
C2 – as of two months ago
C2 #3
(unknown)
C2 – as of today
(Infected, not yet
identified)

#3: Determining the systems that communicated with a specified Internet IP address

- Log firewall “accepts” or NetFlow for outbound traffic
- If the volume of data becomes prohibitive
  - Filter out events associated with the most common legitimate destinations
    - Avoid filtering out ranges associated with open-to-the-public hosting environments, could be used for hosting C2
- Test the scenario where you query this data to identify communications with an IP address
  - Ensure you have DHCP logs and can determine the source host name
- Implement alerting capability

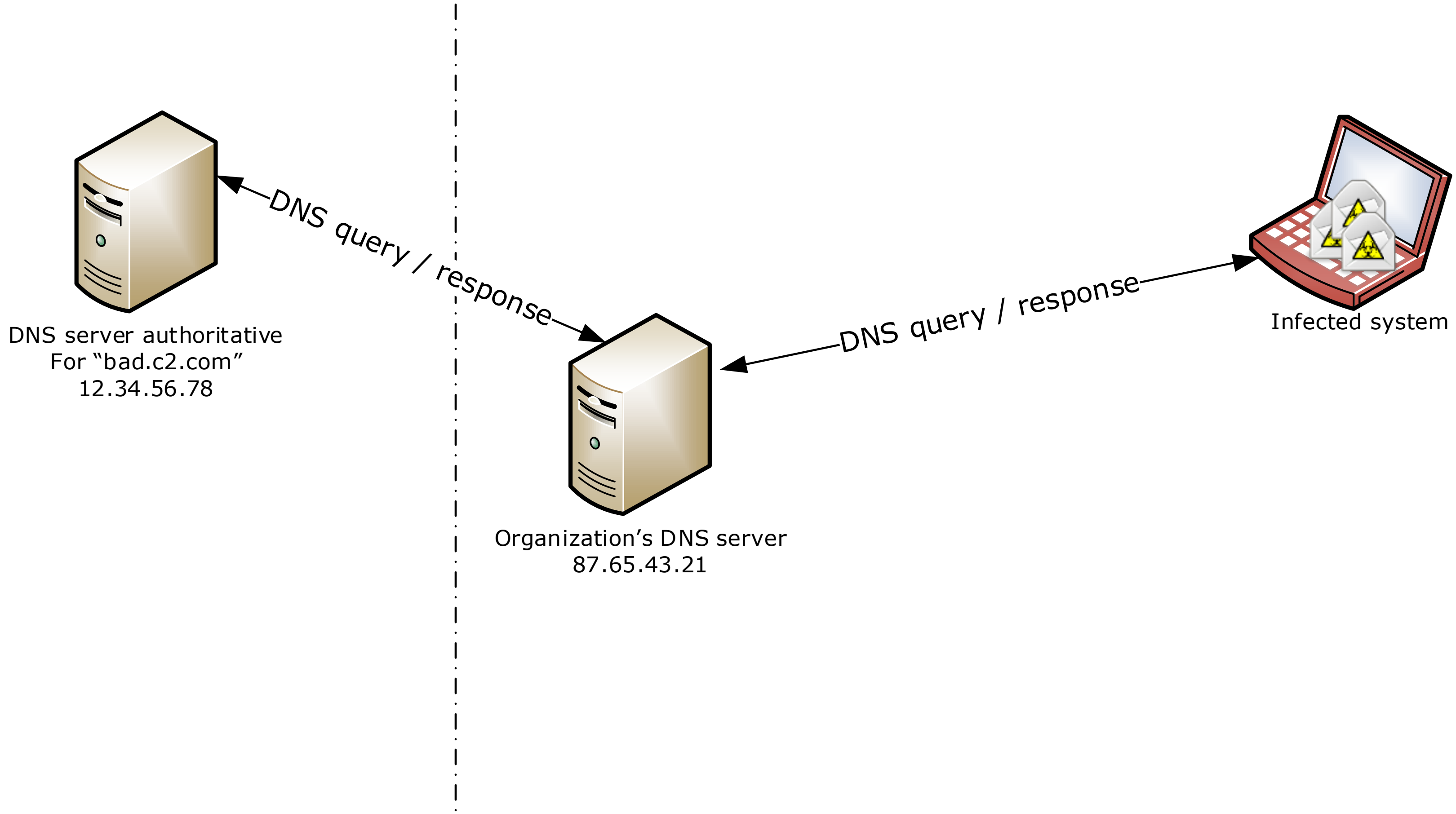

DNS query
C2 FQDN #1
really-bad-net.com =
98.76.54.3



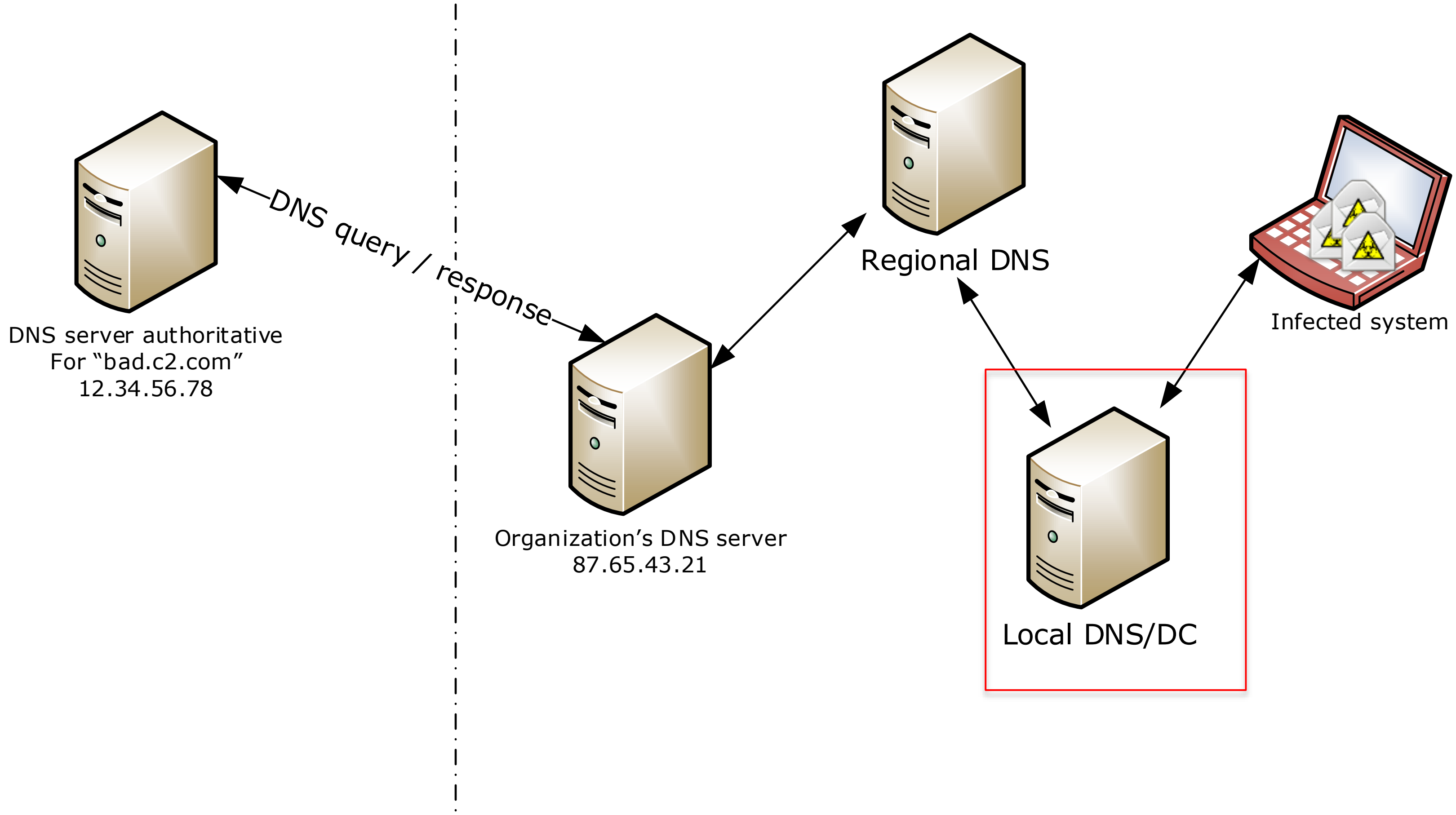
C2 FQDN #2

surreptitious.net = 127.0.0.1

#4: Tracking domain name resolution attempts



#4: Tracking domain name resolution attempts

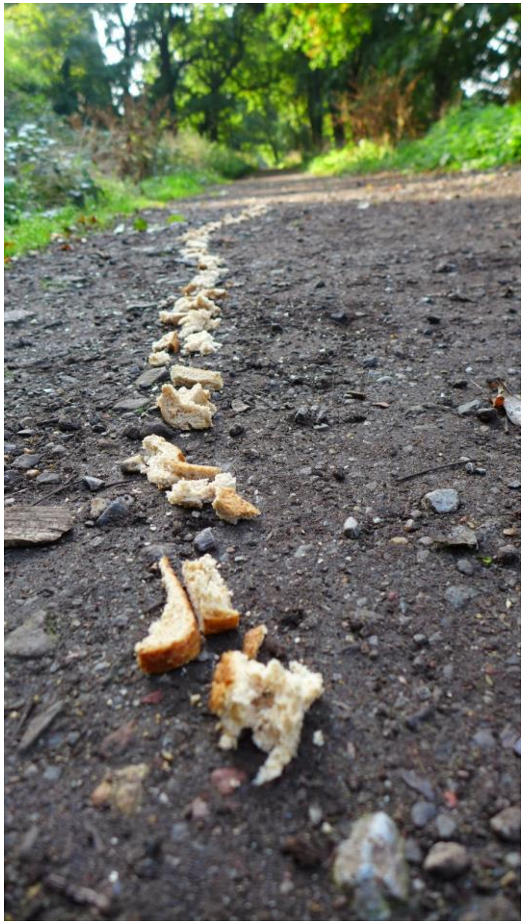


#4: Tracking domain name resolution attempts

- Easier to log at the proxy
  - Blind spot
- If the volume of data becomes prohibitive
  - Filter out events associated with internal name lookups and top known-good domains
- Block resolution of dynamic DNS names

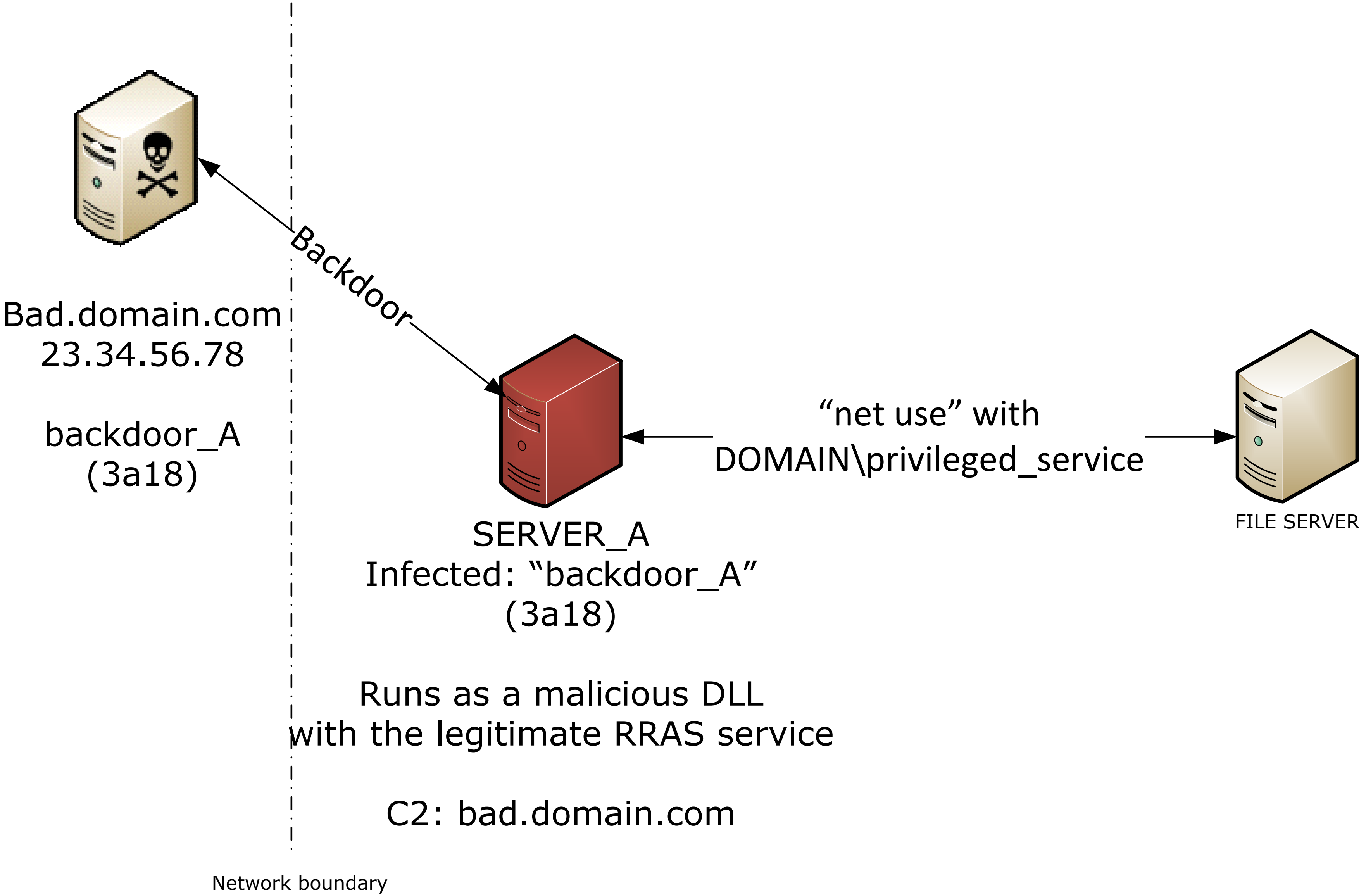
#5: Identifying indicators of compromise across the environment

- Host-based or network-based artifacts
- May be artifacts associated with a specific attacker or intrusion
- May be general conditions indicating malicious activity
- Use cases for codifying IOCs:
  - Find malware or utilities
  - Methodology
  - Bulk
  - Investigative



*For additional details visit: https://www.mandiant.com/blog/openioc-basics/

- Antivirus
- System/configuration management software
- NIDS
- SIEM
- Vulnerability scanners
- PowerShell/WMI



Bad.domain.com
23.34.56.78

backdoor_A
(3a18)

Backdoor

SERVER_A
Infected: "backdoor_A"
(3a18)

Runs as a malicious DLL
with the legitimate RRAS service

C2: bad.domain.com

"net use" with
DOMAIN\privileged_service

FILE SERVER

Network boundary

- Network-based indicators (NBIs)
  - Successful packets destined for 23.34.56.78.
  - DNS query for “bad.domain.com”.
  - Patterns specific to the backdoor’s C2 protocol.
- Host-based indicators (HBIs)
  - The system has an established TCP connection to 23.34.56.78.
  - The system’s DNS cache contains “bad.domain.com”.
  - Security event logs contain a successful authentication event by the “DOMAIN\privileged_service” account, or from SERVER_A during known periods of activity.
  - The registry key for any service DLL file name contains “sneaky.dll”.

- More HBIs:
    - A file has the MD5 hash 3a185c77d533d12544bfc6a24d7d2a75 (matches the malicious service DLL).
    - A file was compiled on December 4, 2013 at 05:22:13 UTC and has a size of 20,241 bytes (may catch variants of the malicious service DLL that are very similar, but not exactly a hash match).
    - An executable or DLL imports from “ws2_32.dll” and also imports all of the following functions: “RegisterServiceCtrlHandlerA”, “RegQueryValueExA”, “OpenServiceA”, “InitSecurityInterfaceA” (may catch variants of the malicious service DLL, but will likely have false positive hits).
    - A running process has a mutex named “733f0_fd3t” (may catch other pieces of malware by the same author, who may prefer to use this name for a mutex).

Conclusions

- Develop IR use cases, conduct simulations
  - Determine what capabilities _you_ need in your environment for the types of threats you face
- Define requirements for new roles, processes, and tools
- Ensure you are measuring something useful
  - Mean-time-to-remediate
  - Mean-time-to-detect

Contact information:

- E-mail:

  Jim.Aldridge@Mandiant.com

- Twitter:

  @jimaldridge

- Mandiant:

  www.mandiant.com