HW11 Network Security

– Ralph Pursifull

Part 1: Review Questions

Security Control Types

The concept of defense in depth can be broken down into three different security control types. Identify the security control type of each set of defense tactics.

1. Walls, bollards, fences, guard dogs, cameras, and lighting are what type of security control?

   physical

2. Security awareness programs, BYOD policies, and ethical hiring practices are what type of security control?

   administrative

3. Encryption, biometric fingerprint readers, firewalls, endpoint security, and intrusion detection systems are what type of security control?

   technical

Intrusion Detection and Attack indicators

1. What's the difference between an IDS and an IPS?

   IDS are passive. They detect and log information, but do not respond.
   IPS are active. They go beyond detection to block suspicious activity.

2. What's the difference between an Indicator of Attack (**IOA**) and an Indicator of Compromise (**IOC**)?

   An IOA indicates an attack is happening in real time.
   An IOC indicates previous malicious activity has occurred, resulting in a breach

The Cyber Kill Chain

Name each of the seven stages for the Cyber Kill chain and provide a brief example of each.

Stage 1: **Reconnaissance -** Attackers gather information. Could be harvesting email addresses, conference information… Goal is to determine: “What does the victim have that can be sold or held for ransom?”

Stage 2: **Weaponization -** Attackers develop a malicious payload for the victim. Bad guys make a plan and develop tools or methods required by their plan.

Stage 3: **Delivery -** Attackers launch their intrusion. Bad guys put the plan in motion, by delivering the weaponized bundle to the victim's environment.

Stage 4: **Exploitation -** Attackers compromise their target. The weaponized bundle is activated. In the case of ransomware, this could be the beginning of encryption of critical data.

Stage 5: **Installation -** Attackers gain persistence. Here attackers do what is needed to ensure their weaponized payload will survive a simple reboot or other obvious first steps at removal.

Stage 6: **Command and Control -** Attackers issue commands to their payload. Bad guys are now issuing new instructions to the weaponized payload, perhaps to put pressure on them to pay a ransom.

Stage 7: **Actions on Objectives -** Attackers complete their end goal. Here the attackers get what they came for. Perhaps the ransom is paid or sensitive information is sold on the darknet.

Snort Rule Analysis

Use the Snort rule to answer the following questions:

Snort Rule #1

alert tcp $EXTERNAL_NET any -> $HOME_NET 5800:5820 (msg:"ET SCAN Potential VNC Scan 5800-5820"; flags:S,12; threshold: type both, track by_src, count 5, seconds 60; reference:url,doc.emergingthreats.net/2002910; classtype:attempted-recon; sid:2002910; rev:5; metadata:created_at 2010_07_30, updated_at 2010_07_30;)

1. Break down the Sort Rule header and explain what is happening.

alert: this is an ALERT, so higher priority than LOG or PASS.
tcp $EXTERNAL_NET any -> $HOME_NET 5800:5820 consider tcp from outside the network, from any port bound for any internal IP, ports 5800-5820 (used by VNC)
(msg: "ET SCAN Potential VNC Scan 5800-5820"; so warn of a VNC port scan
NOTE: "flow" flag is not listed, so not looking at flow of traffic… this is just 1 packet
flags:S,12; TCP flags are SYN, FIN, PSH, URG, RST or ACK. **SYN + 2 reserved bits are set**
threshold: type both, track by_src, count 5, seconds 60;
To reduce alarms, Alert once per 60 seconds after seeing 5 events from this source
reference:url,doc.emergingthreats.net/2002910; see this URL for more on this attack
classtype:attempted-recon; this probe of VNC is classified as attempted reconnaissance.
sid:2002910; Snort ID for this event is 2002910

rev:5; This is revision 5 of the rule.
metadata:created_at 2010_07_30, updated_at 2010_07_30;) info about history of this rule

2. What stage of the Cyber Kill Chain does this alert violate?

   This is Reconnaissance. It is a straightforward port scan probably probing for ways to get inside then look around and see what they can find.

3. What kind of attack is indicated?

   A scan of ports commonly used for VNC has generated this Indicator of Attack (IOA). Some bad guy wants a VNC password prompt, hoping to gain access to someone's VNC desktop. So this is the early stage of a password attack.

Snort Rule #2

alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET POLICY PE EXE or DLL Windows file download HTTP"; flow:established,to_client; flowbits:isnotset,ET.http.binary; flowbits:isnotset,ET.INFO.WindowsUpdate; file_data; content:"MZ"; within:2; byte_jump:4,58,relative,little; content:"PE|00 00|"; distance:-64; within:4; flowbits:set,ET.http.binary; metadata: former_category POLICY; reference:url,doc.emergingthreats.net/bin/view/Main/2018959; classtype:policy-violation; sid:2018959; rev:4; metadata:created_at 2014_08_19, updated_at 2017_02_01;)

1. Break down the Sort Rule header and explain what is happening.

alert this is an ALERT, so higher priority than LOG or PASS.
tcp $EXTERNAL_NET $HTTP_PORTS -> from external webservers via TCP
$HOME_NET any to any internal device
(msg:"ET POLICY PE EXE or DLL Windows file download HTTP";
a Windows EXE or DLL is being downloaded to an internal device over HTTP
flow:established,to_client; on an established TCP connection, to the client
flowbits:isnotset,ET.http.binary; if this flow is not already detected (below) ET.http.binary
flowbits:isnotset,ET.INFO.WindowsUpdate; if not part of ET.INFO.WindowsUpdate
file_data; content:"MZ"; with magic bytes "MZ" in the file
within:2; byte_jump:4,58,relative,little; in a certain place, and "PE" a plus or minus
content:"PE|00 00|"; distance:-64; within:4; to identify an executable
flowbits:set,ET.http.binary; set this - to prevent retriggering this rule on same flow
metadata: former_category POLICY;
reference:url,doc.emergingthreats.net/bin/view/Main/2018959; see this URL for more
classtype:policy-violation; classify this as a policy violation
sid:2018959; Snort ID for this event is 2018959 (local)
rev:4; This is revision 4 of this rule
metadata:created_at 2014_08_19, updated_at 2017_02_01;) info about history of this rule

2. What layer of the Defense in Depth model does this alert violate?

   Application layer - An application, here an internet browser, is being used perhaps innocently, to download suspicious files. Perhaps an external website visited by an internal user has been hacked and is being used to spread malware.

   In the Cyber Kill Chain this is **DELIVERY**. A weaponized bundle is being deployed via the web.

3. What kind of attack is indicated?

   Malicious Download

Snort Rule #3

- Your turn! Write a Snort rule that alerts when traffic is detected inbound on port 4444 to the local network on any port. Be sure to include the msg in the Rule Option.

  alert tcp $EXTERNAL_NET 4444 -> $HOME_NET any (msg:"POLICY Inbound traffic from External METASPLOIT port"; classtype:policy-violation; sid:1000001; rev:1; metadata:created_at 2021_11_21)

  --NOTE-- local sid should be numbered above 1,000,000.
  --NOTE-- Port 4444 is the default listening port for Metasploit.
  It could be other things but this port is often used for malicious purposes.

Part 2: "Drop Zone" Lab

Log into the Azure firewalld machine

Log in using the following credentials: Username: sysadmin Password: cybersecurity

Uninstall ufw

Before getting started, you should verify that you do not have any instances of ufw running. This will avoid conflicts with your firewalld service. This also ensures that firewalld will be your default firewall.

- Run the command that removes any running instance of ufw.

```
$ sudo systemctl stop    ufw.service
$ sudo systemctl disable ufw.service
$ sudo systemctl mask    ufw.service
$ sudo ufw  status   # Should say  "Status:inactive"
```

Enable and start firewalld

By default, this service should be running. If not, then run the following commands:

Run the commands that enable and start firewalld upon boots and reboots.
Note: This will ensure that firewalld remains active after each reboot.

```
$ sudo systemctl unmask firewalld.service
$ sudo systemctl enable firewalld.service
$ sudo systemctl start  firewalld.service
```

Confirm that the service is running.

Run the command that checks whether or not the firewalld service is up and running.

```
$ sudo firewall-cmd --state       # to confirm. Should say "running"
$ sudo system status firewalld.service  # Should say "active (running)"
```

List all firewall rules currently configured.

Next, lists all currently configured firewall rules. This will give you a good idea of what's currently configured and save you time in the long run by not doing double work.

Run the command that lists all currently configured firewall rules:

```
$ sudo firewall-cmd --list-all-zones
block         # Note that only the zone "home" has a defined interface
  target: %%REJECT%%
  icmp-block-inversion: no
  interfaces:
  sources:
  services:
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:

dmz
  target: default
  icmp-block-inversion: no
  interfaces:
  sources:
  services: ssh
```

```
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:

drop
  target: DROP
  icmp-block-inversion: no
  interfaces:
  sources:
  services:
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:

external
  target: default
  icmp-block-inversion: no
  interfaces:
  sources:
  services: ssh
  ports:
  protocols:
  masquerade: yes
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:

home (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth0
  sources:
  services: ssh mdns samba-client dhcpv6-client
  ports:
  protocols:
  masquerade: no
```

```
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:

internal
  target: default
  icmp-block-inversion: no
  interfaces:
  sources:
  services: ssh mdns samba-client dhcpv6-client
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:

public
  target: default
  icmp-block-inversion: no
  interfaces:
  sources:
  services: ssh dhcpv6-client
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:

trusted
  target: ACCEPT
  icmp-block-inversion: no
  interfaces:
  sources:
  services:
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
```

```
  rich rules:

work
  target: default
  icmp-block-inversion: no
  interfaces:
  sources:
  services: ssh dhcpv6-client
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:

$ sudo firewall-cmd --get-default-zone
home
$ sudo firewall-cmd --get-active-zones       # Only 1 zone has a nic!
home
  interfaces: eth0      #  So "home" is the only active zone.
```

Used HyperV to add 3 more nics to this VM. All Nics are connected to the Default-Switch.

Take note of what Zones and settings are configured. You may need to remove unneeded services and settings.

List all supported service types that can be enabled.

- Run the command that lists all currently supported services to see if the service you need is available

```
$ sudo firewall-cmd --get-services
RH-Satellite-6 amanda-client amanda-k5-client bacula bacula-client bgp
bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc ceph ceph-mon
cfengine condor-collector ctdb dhcp dhcpv6 dhcpv6-client dns
docker-registry docker-swarm dropbox-lansync elasticsearch freeipa-ldap
freeipa-ldaps freeipa-replication freeipa-trust ftp ganglia-client
ganglia-master git high-availability http https imap imaps ipp ipp-client
ipsec irc ircs iscsi-target kadmin kerberos kibana klogin kpasswd kprop
kshell ldap ldaps libvirt libvirt-tls managesieve mdns minidlna mosh
mountd ms-wbt mssql murmur mysql nfs nfs3 nrpe ntp openvpn ovirt-imageio
ovirt-storageconsole ovirt-vmconsole pmcd pmproxy pmwebapi pmwebapis pop3
pop3s postgresql privoxy proxy-dhcp ptp pulseaudio puppetmaster quassel
radius redis rpc-bind rsh rsyncd samba samba-client sane sip sips smtp
smtp-submission smtps snmp snmptrap spideroak-lansync squid ssh synergy
```

```
syslog syslog-tls telnet tftp tftp-client tinc tor-socks
transmission-client vdsm vnc-server wbem-https xmpp-bosh xmpp-client
xmpp-local xmpp-server zabbix-agent zabbix-server
```

- We can see that the Home and Drop Zones are created by default.

Zone Views

- Run the command that lists all currently configured zones.

```
$ sudo firewall-cmd --get-zones
block dmz drop external home internal public trusted work
```

- We can see that the Public and Drop Zones are created by default. Therefore, we will need to create Zones for Web, Sales, and Mail.

Create Zones for Web, Sales and Mail.

Run the commands that creates Web, Sales and Mail zones.

```
$ sudo firewall-cmd --permanent --new-zone=web
success
$ sudo firewall-cmd --permanent --new-zone=sales
success
$ sudo firewall-cmd --permanent --new-zone=mail
success
$ sudo firewall-cmd --reload
succes
```

Set the zones to their designated interfaces:

Run the commands that sets your eth interfaces to your zones.

```
$ sudo firewall-cmd --zone=public --change-interface=eth0
The interface is under control of NetworkManager, setting zone to
'public'.
success
$ sudo firewall-cmd --zone=web --change-interface=eth1
The interface is under control of NetworkManager, setting zone to
'web'.
success
$ sudo firewall-cmd --zone=sales --change-interface=eth2
The interface is under control of NetworkManager, setting zone to
'sales'.
success
$ sudo firewall-cmd --zone=mail --change-interface=eth3
The interface is under control of NetworkManager, setting zone to
'mail'.
```

```
success
$ sudo firewall-cmd --get-active-zones
mail
  interfaces: eth3
public
  interfaces: eth0
sales
  interfaces: eth2
web
  interfaces: eth1
$ sudo firewall-cmd --set-default-zone=public
success
$ sudo firewall-cmd --runtime-to-permanent
success
$ sudo firewall-cmd --get-default-zone
public
```

Add services to the active zones:

- Run the commands that add services to the **public** zone, the **web** zone, the **sales** zone, and the **mail** zone.

Public:

```
$ sudo firewall-cmd --permanent --zone=public --add-service=http
success
$ sudo firewall-cmd --permanent --zone=public --add-service=https
success
$ sudo firewall-cmd --permanent --zone=public --add-service=pop3
success
$ sudo firewall-cmd --permanent --zone=public --add-service=smtp
success
$ sudo firewall-cmd --permanent --zone=public --remove-service=ssh
success
$ sudo firewall-cmd --permanent --zone=public \
      --remove-service=dhcpv6-client
success
$ sudo firewall-cmd --reload
success
```

Web:

```
$ sudo firewall-cmd --permanent --zone=web --add-service=http
success
$ sudo firewall-cmd --reload
success
```

Sales

```
$ sudo firewall-cmd --permanent --zone=sales --add-service=https
success
$ sudo firewall-cmd --reload
success
```

Mail

```
$ sudo firewall-cmd --permanent --zone=mail --add-service=smtp
success
$ sudo firewall-cmd --permanent --zone=mail --add-service=pop3
success
$ sudo firewall-cmd --reload
success
```

- What is the status of http, https, smtp and pop3?

```
$ sudo firewall-cmd --zone=public --permanent --list-services
http https pop3 smtp
$ sudo firewall-cmd --zone=web    --permanent --list-services
http
$ sudo firewall-cmd --zone=sales  --permanent --list-services
https
$ sudo firewall-cmd --zone=mail   --permanent --list-services
smtp pop3
```

Add your adversaries to the Drop Zone.

Run the command that will add all current and any future blacklisted IPs to the Drop Zone.

```
$ sudo firewall-cmd --zone=drop --permanent --add-source=138.138.0.3
success
$ sudo firewall-cmd --zone=drop --permanent --add-source=10.208.56.23
success
$ sudo firewall-cmd --zone=drop --permanent --add-source=135.95.103.76
success
$ sudo firewall-cmd --zone=drop --permanent --add-source=76.34.169.118
success
$ sudo firewall-cmd --reload
success
```

Associate source IPs with zones, where possible

```
$ sudo firewall-cmd --zone=web  --permanent --add-source=201.45.34.126
success
$ sudo firewall-cmd --zone=sales --permanent --add-source=201.45.15.48
success
```

```
$ sudo firewall-cmd --zone=mail --permanent --add-source=201.45.105.12
success
$ sudo firewall-cmd --reload
success
```

Make rules permanent then reload them:

It's good practice to ensure that your firewalld installation remains nailed up and retains its services across reboots. This ensure that the network remains secured after unplanned outages such as power failures.

- Run the command that reloads the firewalld configurations and writes it to memory

This command writes the runtime configuration to PERMANENT

```
$ sudo firewall-cmd --runtime-to-permanent
```

This one deploys the PERMANENT configuration to the runtime environment

```
$ sudo firewall-cmd --reload
```

View active Zones

Now, we'll want to provide truncated listings of all currently **active** zones. This a good time to verify your zone settings.

- Run the command that displays all zone services

1. First here are the active zones

```
$ sudo firewall-cmd --get-active-zones
drop
  sources: 138.138.0.3 10.208.56.23 135.95.103.76 76.34.169.118
mail
  interfaces: eth3
  sources: 201.45.105.12
public
  interfaces: eth0
sales
  interfaces: eth2
  sources: 201.45.15.48
web
  interfaces: eth1
  sources: 201.45.34.126
```

2. Here are the services available for each active zone

```
$ sudo firewall-cmd --zone=public --permanent --list-services
http https pop3 smtp
$ sudo firewall-cmd --zone=sales --permanent --list-services
https
$ sudo firewall-cmd --zone=web --permanent --list-services
http
$ sudo firewall-cmd --zone=mail --permanent --list-services
smtp pop3

So we are close.
```

Block an IP address

- Use a rich-rule that blocks the IP address 138.138.0.3.

```
# first take it out of the drop zone

$ sudo firewall-cmd --zone=drop --permanent      \
         --remove-source=138.138.0.3

# now put it in public

$ sudo firewall-cmd --permanent --zone=public --add-rich-rule='rule  \
      family=ipv4 source address=138.138.0.3 reject'
success
$ sudo firewall-cmd --reload
success
```

Block Ping/ICMP Requests

Harden your network against ping scans by blocking icmp echo replies.

- Run the command that blocks pings and icmp requests in your public zone.

```
$ sudo firewall-cmd --permanent --zone=public     \
        --add-rich-rule='rule protocol value=icmp reject'
success
```

Rule Check

Now that you've set up your brand new firewalld installation, it's time to verify that all of the settings have taken effect.
Run the command that lists all of the rule settings. Do one command at a time for each zone.

```
$ sudo firewall-cmd --list-all --zone=public
```

```
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth0
  sources:
  services: http https pop3 smtp
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
      rule family="ipv4" source address="138.138.0.3" reject
      rule protocol value="icmp" reject

$ sudo firewall-cmd --list-all --zone=web
web (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth1
  sources: 201.45.34.126
  services: http
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:

$ sudo firewall-cmd --list-all --zone=sales
sales (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth2
  sources: 201.45.15.48
  services: https
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

```
$ sudo firewall-cmd --list-all --zone=mail
mail (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth3
  sources: 201.45.105.12
  services: smtp pop3
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:

$ sudo firewall-cmd --list-all --zone=drop
drop (active)
  target: DROP
  icmp-block-inversion: no
  interfaces:
  sources: 10.208.56.23 135.95.103.76 76.34.169.118
  services:
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

- Are all of our rules in place? If not, then go back and make the necessary modifications before checking again.

Looks good to me!

Congratulations! You have successfully configured and deployed a fully comprehensive firewalld installation.

Part 3: IDS, IPS, DiD and Firewalls

Now, we will work on another lab. Before you start, complete the following review questions.

IDS vs. IPS Systems

1. Name and define two ways an IDS connects to a network.
   Answer 1: **Network Intrusion Detection (NIDS)** - A packet sniffer is connected to the network to watch traffic. Could be in a position to watch traffic to/from the internet.
   Answer 2: **Host-based Intrusion Detection (HIDS)** - Processes run locally on valuable systems and send logs to a centralized repository.

2. Describe how an IPS connects to a network.
   Answer: **Intrusion Protection Systems (IPS)** connect inline with the flow of data, typically between the firewall and network switch.

3. What type of IDS compares patterns of traffic to predefined signatures and is unable to detect Zero-Day attacks?
   Answer: **Network Intrusion Detection** is based on signatures of known bad behavior.

4. Which type of IDS is beneficial for detecting all suspicious traffic that deviates from the well-known baseline and is excellent at detecting when an attacker probes or sweeps a network?
   Answer: **Host-based Intrusion Detection** is watching activity on a host computer, so it's better positioned to detect "strange" activity.

Defense in Depth

1. For each of the following scenarios, provide the layer of Defense in Depth that applies:
    1. A criminal hacker tailgates an employee through an exterior door into a secured facility, explaining that they forgot their badge at home.
       Answer: **Perimeter**
    2. A zero-day goes undetected by antivirus software.
       Answer: **Host**
    3. A criminal successfully gains access to HR's database.
       Answer: **Data**
    4. A criminal hacker exploits a vulnerability within an operating system.
       Answer: **Host**
    5. A hacktivist organization successfully performs a DDoS attack, taking down a government website.
       Answer: **Application**
    6. Data is classified at the wrong classification level.
       Answer: **Data**
    7. A state sponsored hacker group successfully firewalked an organization to produce a list of active services on an email server.
       Answer: **Network**

2. Name one method of protecting data-at-rest from being readable on hard drive.
   Answer: **Disk encryption, Bitlocker for example.**

3. Name one method to protect data-in-transit.
   Answer: **TLS, HTTPS, ...**

4. What technology could provide law enforcement with the ability to track and recover a stolen laptop.
   Answer: **Device tracking systems like LoJack for Laptops or EXO5**

5. How could you prevent an attacker from booting a stolen laptop using an external hard drive?
   Answer: **Bitlocker full disk encryption, requiring TPM + PIN to unlock**

Firewall Architectures and Methodologies

1. Which type of firewall verifies the three-way TCP handshake? TCP handshake checks are designed to ensure that session packets are from legitimate sources.
   Answer: **Circuit Level FIrewalls**

2. Which type of firewall considers the connection as a whole? Meaning, instead of looking at only individual packets, these firewalls look at whole streams of packets at one time.
   Answer: **Packet Filtering FIrewalls (Stateful)**

3. Which type of firewall intercepts all traffic prior to being forwarded to its final destination. In a sense, these firewalls act on behalf of the recipient by ensuring the traffic is safe prior to forwarding it?
   Answer: **Application (Proxy) Firewalls**

4. Which type of firewall examines data within a packet as it progresses through a network interface by examining source and destination IP address, port number, and packet type-all without opening the packet to inspect its contents?
   Answer: **Packet Filtering Firewalls (Stateless)**

5. Which type of firewall filters based solely on source and destination MAC address?
   Answer: **MAC Layer Firewall**

Bonus Lab: "Green Eggs & SPAM"

In this activity, you will target spam, uncover its whereabouts, and attempt to discover the intent of the attacker.

- You will assume the role of a Junior Security administrator working for the Department of Technology for the State of California.

- As a junior administrator, your primary role is to perform the initial triage of alert data: the initial investigation and analysis followed by an escalation of high priority alerts to senior incident handlers for further review.

- You will work as part of a Computer and Incident Response Team (CIRT), responsible for compiling **Threat Intelligence** as part of your incident report.

Threat Intelligence Card

Note: Log into the Security Onion VM and use the following **Indicator of Attack** to complete this portion of the homework.

Locate the following Indicator of Attack in Sguil based off of the following:

- **Source IP/Port**: 188.124.9.56:80
- **Destination Address/Port**: 192.168.3.35:1035
- **Event Message**: ET TROJAN JS/Nemucod.M.gen downloading EXE payload

Answer the following:

1. What was the indicator of an attack?

   An attempt to download an EXE file via HTTP from the web server at 188.124.9.56.

   - Hint: What do the details of the reveal?

   Three related campaigns are targeting spam email at Italian users. All three variations use the Javascript downloader named JS/Nemucod. The downloader is inside a Zip file attached to the email. Opening the Zip then double clicking on the Javascript causes the code to be executed by Internet Explorer. After several layered downloads, an information stealer is installed.

2. What was the adversarial motivation (purpose of attack)?

   This is an attempt to deploy the Gozi infostealer at companies in Italy. So the purpose is theft of personal or corporate information.

3. Describe observations and indicators that may be related to the perpetrators of the intrusion. Categorize your insights according to the appropriate stage of the cyber kill chain, as structured in the following table.

TTP	Example	Findings

Reconnaissance	How did the attacker locate the victim?	Finding: Email and Invoice are written in Italian. Conjecture: Perhaps this campaign was focused on email addresses of domains based in Italy or under the ".it" top level domain. Or perhaps the bad guys bought malware and only paid for the right to use it in Italy… (Just kidding about that).
Weaponization	What was it that was downloaded?	When fully successful, the Gozi infostealer is installed..
Delivery	How was it downloaded?	Attached to the email was a ZIP file containing a Javascript downloader named JS/Nemucod.
Exploitation	What does the exploit do?	If a user clicks on the contents of that ZIP, JS/Nemucod will invoke three ActiveX controls: WScript.Shell, MSXML2.XMLHTTP and ADODB.Stream. Ultimately WScript.Shell causes execution of an EXE or DLL that can retrieve a Trojan Downloader called Fareit or Pony Downloader…
Installation	How is the exploit installed?	… then Fareit or Pony Downloader initiates download of the Gozi infostealer.
Command & Control (C2)	How does the attacker gain control of the remote machine?	Gozi makes itself more persistent by copying itself to a file named "xx_????.exe" in the user's directory with the last 4 letters in the new filename randomly generated. It then creates a registry key so the new copy will be run again after a reboot.
Actions on Objectives	What does the software that the attacker sent do to complete it's tasks?	Once fully installed, Gozi would use weaknesses in Internet Explorer, such that every POST request to a legitimate HTTPS website was also sent with HTTP to the Gozi Command and Control system. So credit card information, email dialogs, … are obtained by the hackers.

4. What are your recommended mitigation strategies?

1. Install SNORT rule to detect activity in our detection and prevention systems.

2. Make sure this is reported to law enforcement.

2. Blacklist to the extent possible, the following domains and IPs to prevent further disclosure of information.

dcmyx[.]com	**ibmdatacap[.]com**	**www.landtourjapan[.]com**
thevillageveterinaryhospital[.]com		**majorcase[.]org**
albirtchad[.]org	**czarplast[.]com**	**www.yurtmobilyalari[.]net**
jlinksms[.]com	**alberchad[.]org**	**bugrasilte[.]com**
skbmw[.]com	**wellnessherbal[.]com**	**istanbulklima[.]org**
erikssonelectric[.]com	**sieumaukimdung[.]com**	**www.landtourjapan[.]com**
creativefoodstylist[.]com	**wellnessherbal[.]com**	**belarusstudy[.]com**
adenyaoteleet[.]com	**tripsnepal[.]com**	**famoussuperstars[.]ru**
torpedazil[.]ru	**gofermertoop[.]ru**	**109.120.142[.]168**
109.120.155[.]	**30 83.69.230[.]16**	

3. Alert our user community in Italy.

4. DON'T: Go on underground IRC with the handle: "Gozi"... See who contacts me. Fortunately someone already did that.

5. List your third-party references.

Certego S.R.L, Modena MO, Italy: "Italian spam campaigns using JS/Nemucod downloader"
www.certego.net/en/news/italian-spam-campaigns-using-js-nemucod-downloader

Dell Secureworks, Atlanta, Georgia: "Gozi Trojan" by Don Jackson
https://www.secureworks.com/research/gozi
