Host infected with malware

If you are reading this page, it's most likely because you've received a malware report from us advising you to refer to this page should you require assistance.

Why have you received this report?

Janet CSIRT receive various intelligence feeds of infected or compromised hosts and hosts running vulnerable services accessible from the internet that exist on the Janet network. The report you received may have been generated through connections to one of many sinkholes and monitored command and control servers reporting to the feed providers.

Why should you care?

Whilst the reports show connections to benign sinkholes monitored by security researchers, it is highly likely that the infected host is also connecting to the attackers servers. The infected host could be receiving instructions to carry out attacks on other hosts, sending out spam or exfiltrating data including IP address, hostname, running services, plugin/software versions, usernames, passwords, and much more. It could be spreading itself across the network, infecting network shares and usb storage. If a host is sending out spam, it is likely the outgoing mail relay will to be add to various blacklists affecting mail delivery from your network and institution.

What should you be looking at?

“timestamp”,”ip”,”port”,”asn”,”geo”,”region”,”city”,”hostname”,”type”,”infection”,”url”,”agent”, ”cc”, ”cc_port”, ”cc_asn”,
”cc_geo”,”cc_dns”,”count”,”proxy”,”application”,”p0f_genre”,”p0f_detail”, ”machine_name”,”id”

“2014-11-19 10:52:56”,”123.45.67.89”,56384,786,”UK”,”OXF”,”WITNEY”,”nat-host.example.ac.uk”,,”nethelper”,”/”,”Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:33.0) Gecko/20100101 Firefox/33.0”,”212.227.252.196”,80,8560,”DE”,”212.227.252.196”,1,,,,,,

The hostname may give the user/device away, however that's not often the case. There are 5 key pieces of information that should assist you in identifying either *1) the infected host* or *2) the device owner*:

- Timestamp: 2014-11-19 10:52:56
- Source IP: 123.45.67.89
- Source port: 56384
- Destination IP: 212.227.252.196
- Destination port: 80

This information gives us a start for your investigation. It tells us that at 2014-11-19 10:52:56, source IP 123.45.67.89 created a session using source port 56384 and connected to port 80

on 212.227.252.196. It is likely to be a TCP connection, although some malware uses UDP.

How could you isolate a device based on this information?

You may have a well documented network and know exactly who 123.45.67.89 belongs to. But this may not be the case. In many cases 123.45.67.89 is a public-NAT IP which can be used by many hosts inside your network.

Firewall logs

If you log every connection you will be able to identify the session within your firewall logs:

Nov 19 10:52:56 10.10.20.1 %ASA-6-302013: Built outbound TCP connection 118452310 for ext:212.227.252.196/80 (212.227.252.196/80) to desktop:10.10.25.22/56384 (123.45.67.89/56384)

This not only gives us confirmation that a connection occurred, but it also gives us the inside host IP address (10.10.25.22). You could also find this information in your proxy logs.

DHCP logs

There are various ways to identify the device owner. Search your DHCP logs to find the MAC address which had 10.10.25.22 at the time mentioned in the report. You can then start to think about the following questions:

- Is the host in your domain computers DHCP pool?
    - Your DHCP logs may show the domain name of the computer which may (should!) be assigned to a user in an inventory.
    - Presumably you run a centralised antivirus solution which your domain machines' AV client is tied to, has the machine been flagged as infected?
- Is this an Eduroam user?
    - Search your authentication logs for the Eduroam user authenticating using the MAC address from your DHCP logs.
- Is the IP a VPN user?
    - A VPN connection should log the username authenticated and the IP address it has been assigned.
- Can you trace the MAC address to a particular switch port?
- Does each device MAC address need to be registered with a owner name before accessing the network?
    - With the MAC address in hand, you can then consult your registration database to find the user.
- If you aren't able to tie the MAC address to a particular user.
    - Are you able to block the user by MAC address?
        - Some switches allow you to create MAC address-based access control lists.
        - Most DHCP servers should allow you to create DHCP reservations, maybe put their MAC address into a quarantine VLAN?

Obviously, the information available to you will depend on the operating systems your services run on and the solutions you use for authentication, DHCP, logging, VPN etc.
