Contents

[Welcome 3](#_Toc81307262)

[Exercise 1 – Case Studies 4](#_Toc81307263)

[1.0 Backdoor 4](#_Toc81307264)

[2.0 Lateral movement 4](#_Toc81307265)

[Exercise 2 – Technical Exercise 5](#_Toc81307266)

# Exercise 1 – Case Studies

## Backdoor

A backdoor was found on a machine belonging to a senior HR manager. Further analysis shows that the malicious executable infected the machine about 6 hours ago and that multiple malicious HTTP command and control connections were successfully established with an external domain. Proxy logs show that over 20 MB were transferred to the malicious destination and that the connection is still active.

* + 1. How would you investigate the issue?

In the SANS Incident Response Plan, the six steps to incident response **are preparation, identification, containment, eradication, recovery and lesson learnt**. In this incident, the next step would be to also identify any other devices on the same subnet has been infected, whilst also containing this first device discovered to be infected. This would mean disconnecting the HR manager’s machine from the network, and putting firewalls/IPS rules to block connections to the external domain. Just an example specific to Darktrace’s Enterprise Immune System product, the domain can be added to the Watched Domains list with Antigena applied, which will send TCP resets to the source device to close the connection between it and the external endpoint, in the event any other devices on the network attempt to connect to the malicious C2 server. Depending on the tools available, EDR/NDR tools can also be used to find out potential infections on other devices in the network. Additional investigations, such as inputting the domain/IP into OSINT (e.g. Virustotal, DomainIQ) can also be done to provide more context for the C2 endpoint (e.g. Cobalt Strike C2 server).

* + 1. Your line manager is very concerned about the data sent out and she asks you to find out what type data have been exfiltrated to the malicious C2. How would you proceed?

A PCAP of the connections can be obtained and viewed in Wireshark. If the connections associated with the 20MB data exfiltration are unencrypted, the HTTP requests of interest are most likely those with POST methods. For example, I have seen information stealers using POST requests to endpoints with newly registered domains to exfiltrate ZIP files containing potentially sensitive stolen data. If the connections are encrypted, anomaly detection tools could have detected anomalous data uploads to the domain and also if the data was collected from any other internal devices in downloads. From there, to find out the kind of data stolen, a search for the archive files can be done if they still remain on the computer, else host-based analysis through event log files can be done to see the folder/files gathered. If data was also downloaded from other systems, such as through SMB protocol, NDR tools can be used to see the filenames to identify the exfiltrated documents.

* + 1. How do you make sure that the backdoor is not capable of connecting to other command and control destinations?

Host-based analysis and remediation, such as the running of AV scans can be done to quarantine the malware on the devices. Malware analysis can be done to understand the behaviour and uncover hidden indicators of compromise (IoCs). Thereafter, these IPs/domains can be added to firewall/IPS rules to block such connections.

## Lateral movement

The IDS has identified an attempt to exploit an unpatched HP Loadrunner server originating from IP 10.12.15.45. After investigating the matter, you have confirmed that the IP is associated to a Red Team analyst’s device, who has bypassed your NAC and connected a rogue laptop to the corporate network.

* + 1. What logs sources can you leverage to identify when the device was firstly seen on the network?

Network Access Control is a solution to prevent unauthorized access to internal networks. It restricts access to the network based on the identity or security posture of the device that is trying to connect. DHCP and DNS are some of the logs that can be used. DHCP uses MAC address as the identifier and when the device comes onto the network, the DHCP server would assign an IP address to it (10.12.15.45 in this case). MAC spoofing can be used to bypass NAC. Looking at the DHCP logs on the DHCP server, the datetime when the IP 10.12.15.45 was assigned to the rogue device’s MAC address in the DHCP Ack would be the first seen. DNS is used for the translation of hostnames/domains into IP addresses, which the rogue device would most certainly have used to make connections to other endpoints. DNS logs on the external/internals DNS server can also be examined if DHCP is not available to determine first seen. The network logs related to authentication, such as Kerberos connections to the domain controller, or even SMB connections (e.g. NTLM) can also be used for such tracking.

* + 1. You have now confirmed that the laptop was firstly seen 5 days ago, therefore there is a high chance that the attacker was able to carry out lateral movement. What can be searched in Windows event logs that can indicate lateral movement?

Living off the land techniques, whereby common Windows tools are often used by attackers to blend into the environment and carry out lateral movement. Search for tools such as Powershell, Windows Management Interface (WMI), Windows Command Processor, Windows Based Script Host Console Based Script Host, Task Scheduler Configuration, Scheduled Service Command Line Interface, Service Control Manager Configuration, Whoami and PsExec etc. to find any usual, new or uncommon usage of such tools. Other anomaly detection tools can also be used to spot such suspicious lateral movement in the internal network and reduce the workload on the analyst to spot such new activities.

* + 1. The device was seen connecting to a server over 20,000 times in 10 minutes over port 389/tcp. Is this connectivity expected? What does it indicate?

Port 389 is default port used for LDAP, used as an authentication protocol for directory services. Multiple authentication failures can signify a brute force attempt and such a large number of failed logins definitely indicates something unexpected.

# Exercise 2 – Technical Exercise

While responding to an incident, you have been provided with a packet capture of suspicious activity from a host. You have reason to believe that a user has been taking part in malware distribution campaigns and uploaded malicious files to a server. Thankfully, the GSOC was able to rapidly respond to the incident and isolate the machine. You have been tasked with examining the packet capture to develop a timeline of the incident.

* + 1. What is the IP address of the source machine that uploaded the file?

192.169.10.111 (private IP address)

* + 1. What is the destination IP address of the file upload?

178.128.25.67 (public IP address)

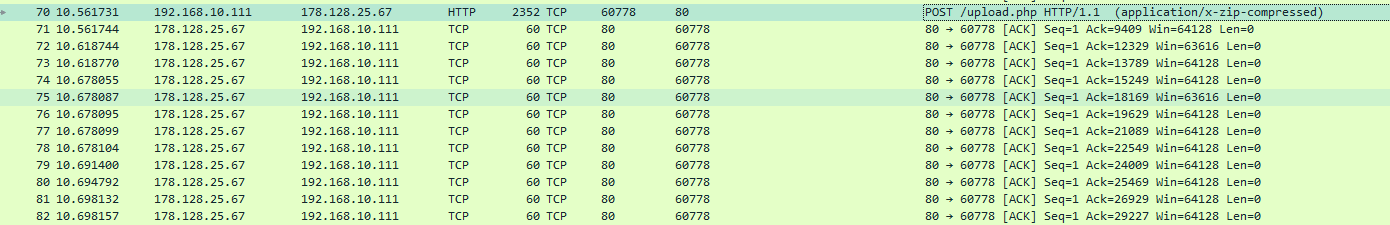
* + 1. What is the name of the file uploaded?

upload.php > Resume-2021.zip > Resume John Doe.doc

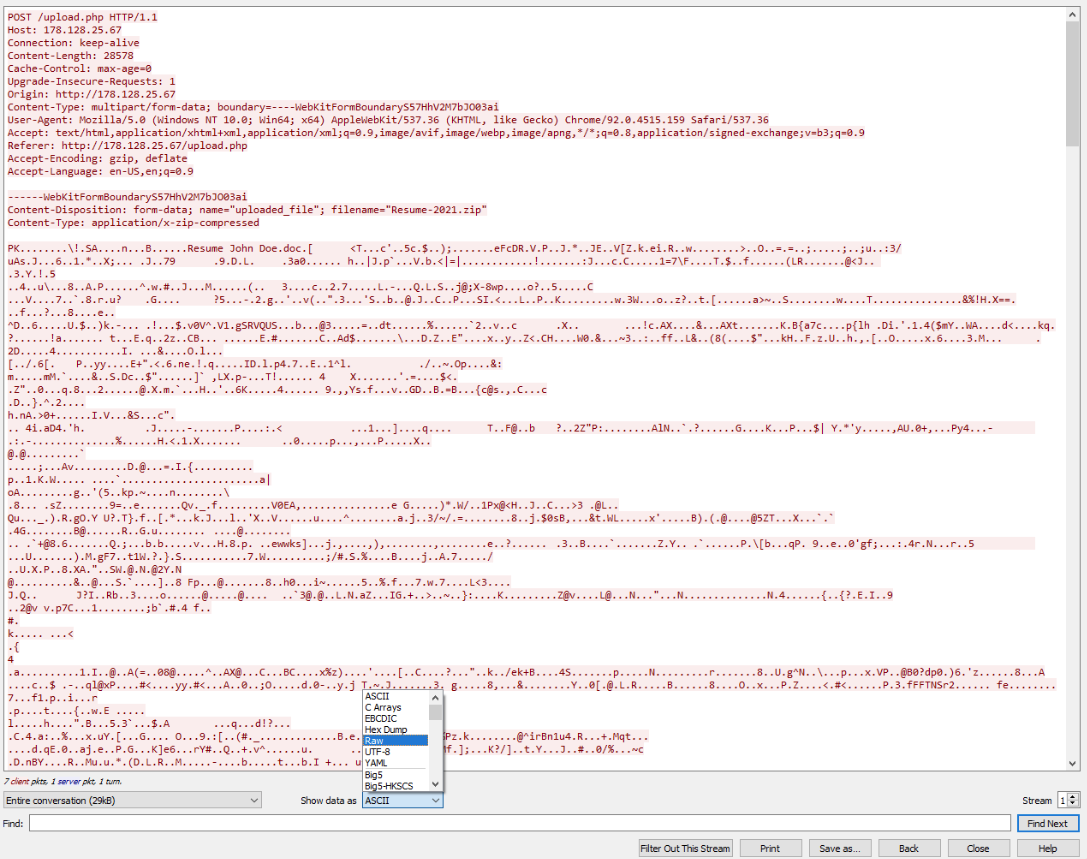
* + 1. What is the MD5 hash of the file uploaded to the server?

Steps:

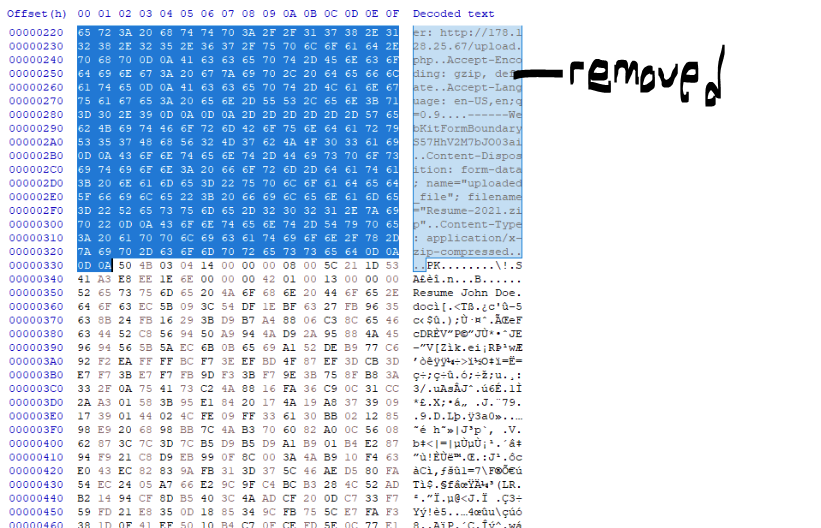
1. First, I followed the TCP/HTTP stream of the HTTP POST with the ZIP file.

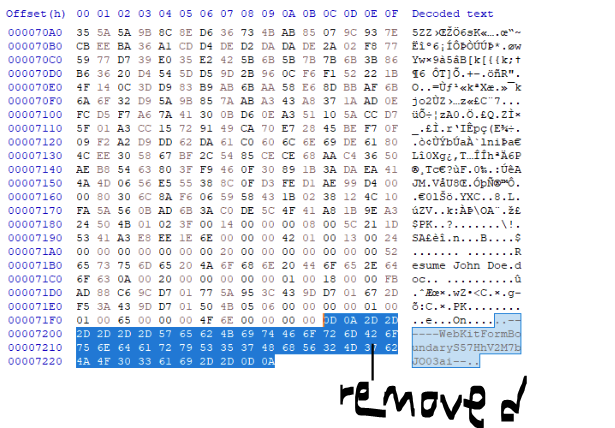


1. I saved the following result as RAW data

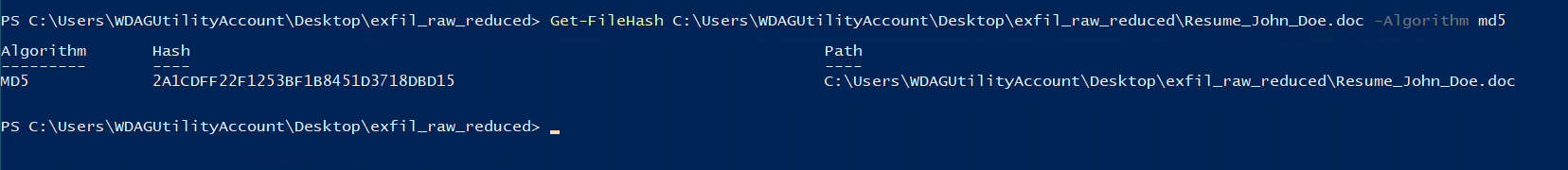


1. Next I used a hex editor to remove the HTTP request portions/body (with hex OD OA) at the start and end so that the only the ZIP file portion remains (starting with ’PK’)





1. Saved the remaining hex as a ZIP file. Doc file can be opening in Windows Sandbox after extracting the ZIP file. Go into PowerShell, and getting the hash by running the below command.



**MD5 hash - 2A1CDFF22F1253BF1B8451D3718DBD15**

* + 1. What course did John Doe study at University?

B.S Astronomy at University of Pluto

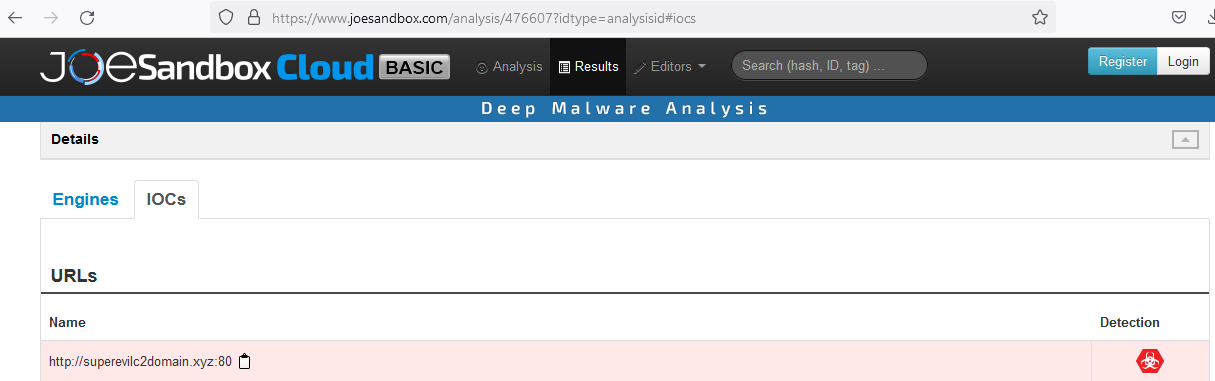


* + 1. What C2 address does the malware communicate to?

superevilc2domain[.]xyz (registered recently 8 months ago – suspicious)

* + 1. Explain the process you took to discover the C2 address.

In Windows Sandbox, upload the Resume John Doe.doc file onto Virustotal. In the community section, sandbox analysis has already been done. By visiting the Joe Sandbox link and going to IoCs tab, the C2 address can be found.



* + 1. Bonus question: Explain the methods the malware uses to execute the malicious code.

A Microsoft Office file that contains the AutoOpen Macro function is used. Macros run automatically whenever the document is opened, executing code and infecting the device.

* + 1. Bonus question: What tool has been leveraged to generate the malware?

Visual Basic Application, VBScript

--- End of Document ---