

## Cheat Sheet

1. What is the full user agent string that uploaded the malicious link file to OneDrive?

Query: index=botsv3 sourcetype=ms:o365:management Workload=OneDrive

Operation=FileUploaded

```
| rename UserID AS user ClientIP AS src_ip SourceFileName AS object  
| table _time UserAgent user src_ip Operation object  
| sort by +time
```

2. What was the name of the macro-enabled attachment identified as malware?

Query: index=botsv3 sourcetype=stream:smtp \*alert\*

3. What is the name of the executable that was embedded in the malware?

Query: index=botsv3 sourcetype=XmlWinEventLog:Microsoft-Windows-Sysmon/Operational \*xlsm\* | sort by +\_time

4. What is the password for the user that was successfully created by the user "root" on the on-premises Linux system?

Query: index=botsv3 host=hoth (adduser OR useradd)

And then index=botsv3 host=hoth (adduser OR useradd) sourcetype="osquery:results"

5. What is the name of the user that was created after the endpoint was compromised?

Query: index=botsv3 source=wineventlog:security EventCode=4720

6. Based on the previous question, what groups was this user assigned to after the endpoint was compromised?

Query: index=botsv3 sourcetype=wineventlog:security svcvnc EventCode=4732

7. What is the process ID of the process listening on a "leet" port?

Query: index=botsv3 1337 sourcetype="osquery:results"

index=botsv3 1337 sourcetype="osquery:results" "columns.port"=1337

8. What is the MD5 value of the file downloaded to Fyodor's endpoint system and used to scan Frothly's network?

Query: index=botsv3 sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" host="FYODOR-L" ("EventID>1</EventID>" OR EventCode=1 OR EventID=1)  
| rex field=\_raw "Data Name='Image'>(?<Image>[^<]+)"  
| rex field=\_raw "Data Name='Hashes'>(?<Hashes>[^<]+)"  
| search Image="\*hdoor.exe"  
| rex field=Hashes "MD5=(?<MD5>[A-Fa-f0-9]{32})"  
| table \_time Image MD5 Hashes