**MALWARE ANALYSIS RUN BOOK**

Deleted

Not Deleted/Not Quarantined

1. Email - If Email was the RC- Purge the email using knowbe4, block the sender on email gateway and block the Ip on F/w.
2. If URL was the RC- Block the URL on Proxy/webgatway.
3. If USB- Educate the user

Manually remove the malware and rescan the host

1. Identify the source of the malware

* Check for email received by the user 2-4 hours before malware detection
* Check all the website the user has visited in last 1 hour
* Check the possibility of malware detection on USB

1. Research on malware
2. Check if the file hash appears elsewhere in network
3. Raise an incident to manually remove the malware
4. Continue analysis & keep adding notes to incident
5. Check if AV has up-to-date signatures
6. Check for any file modification, registry modification, user account creations, privilege escalation and audit logs of affected host

AV ACTION

MALWARE ALERT

GATHER  
INFORMATION

\*Host Name \* File Path \* File hash

\*User \* Malware name \* AV action

\*File name \* Malware category