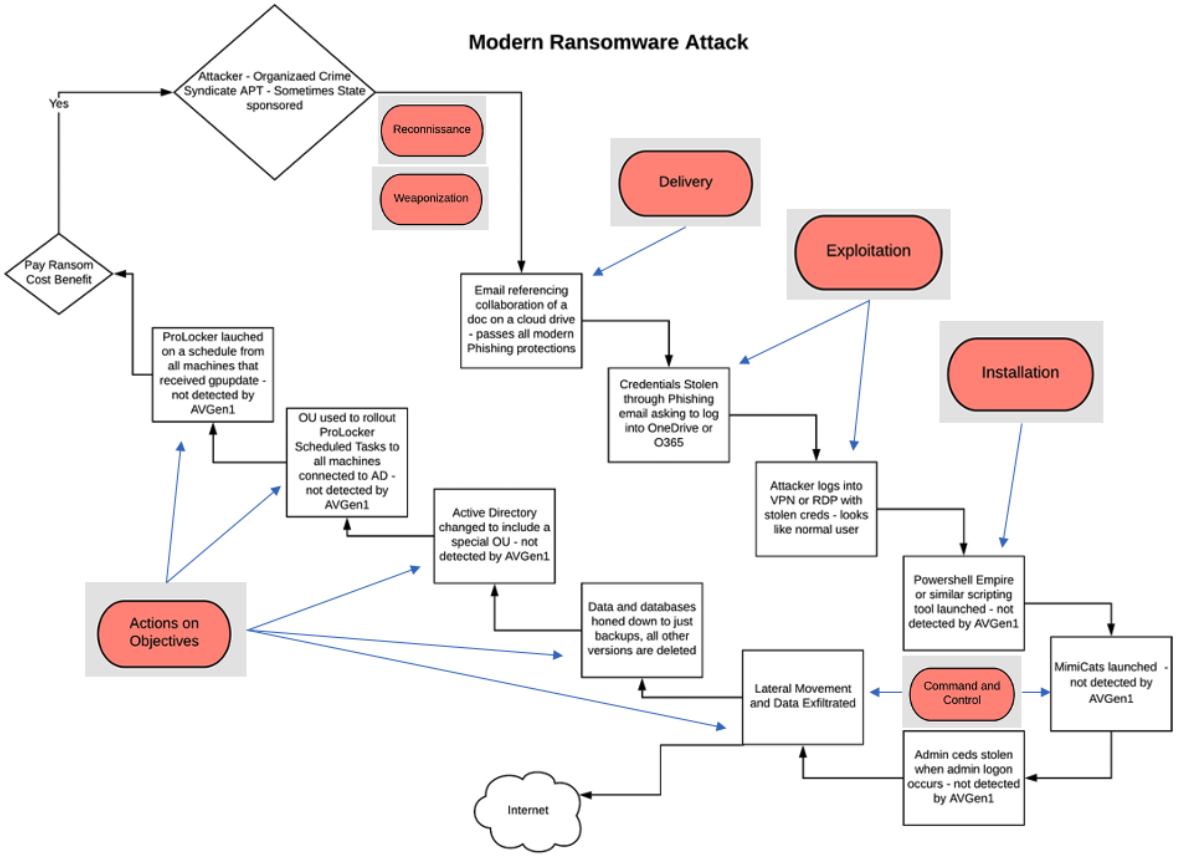

Recon

1. Scanning of your network and cloud assets.
2. Emails phishing for information.
3. Strange phones calls phishing for information.

Delivery

1. Phishing emails with actionable items.
2. Phone calls with actionable items.
3. Scanning of specific ports or an abundance of scanning on a particular port or set of ports or IPs.
4. Brute force authentication requests on external exposed services.

Exploitation

1. Logins or attempted logins at strange times - user heuristics.
2. Impossible travel logins from other geographic locations.
3. Logins or attempted logins from new or unknown IP.
4. Strange IPs or DNS request originating from inside your network or cloud resources.
5. Persistent connections to new or unknown IPs.

Installation

1. Scripting running from non-IT resources.
2. Unknown scripts running in environment.
3. Persistent connections to unknown IPs.

4. Creation of new AD accounts.
5. Elevation of current AD accounts.
6. Use of service accounts for other tasks out of the norm.
7. Logs showing East to West RDP connections IDs (Windows Log Event ID) 1146, 1147, 1148, 1149, 4624 & 4625 Type 3, if out of the norm.

Command and Control

1. Unknown or abnormal DNS requests.
2. Persistent connections to unknown IPs.
3. Large or sustained data flows out of your network of cloud resources.
4. Use of service accounts for other tasks out of the norm.
5. Creation of new AD accounts.
6. Logins or attempted logins at strange times - user heuristics.
7. Impossible travel logins from other geographic locations.
8. Logins or attempted logins from new or unknown IP.

Actions on Objectives

1. Historical backup deletion.
2. Historical database deletion.
3. Unexpected backup changes.
4. Unexpected database changes.
5. Unexpected AD changes especially new OUs or changes to Group Policy.
6. Any IoCs from the Command-and-Control phase can also occur here.