Active Directory Protection
Certes

Summary

A ransomware attack has a distinct pattern and typically follows the seven stage "Kill Chain"

1. **Recon** – Gather Intelligence about a target network
2. **Delivery** – Malware sent to target system
3. **Exploitation** – Malware executed on target system
4. **Privilege Escalation and Lateral Movement** – Gains full control with Admin level privileges
5. **Data Exfiltration** – "Double Extortion" Steal sensitive data before encrypting local copy
6. **Encryption** – Render data inaccessible to Victim
7. **Extortion and Ransom demand** – Demand payment to restore access.

Breaking the "Kill Chain"

- The critical stage in the "Kill Chain" is stage 4 – "Privilege escalation and Lateral movement".
- This is the stage where an attacker moves through the network, having previously gained access via malware / phishing / Zero Day attack, trying to identify where the Domain controllers are, that will enable them to escalate their security privilege to allow them to move to stages 5 – 7.
- Breaking the "Kill Chain" at this stage is critical – Traditional Network Security combined with the use of legitimate domain control admin tools in a "Living-off-the-land" attack are failing to prevent this resulting in the growth of Data breaches.
- Certes – DPRM (Data Protection and Risk Mitigation) approaches this problem from a Data security rather than Network security position.
- DPRM can protect against Ransomware and Data exfiltration by breaking the "Kill Chain".

certes.ai

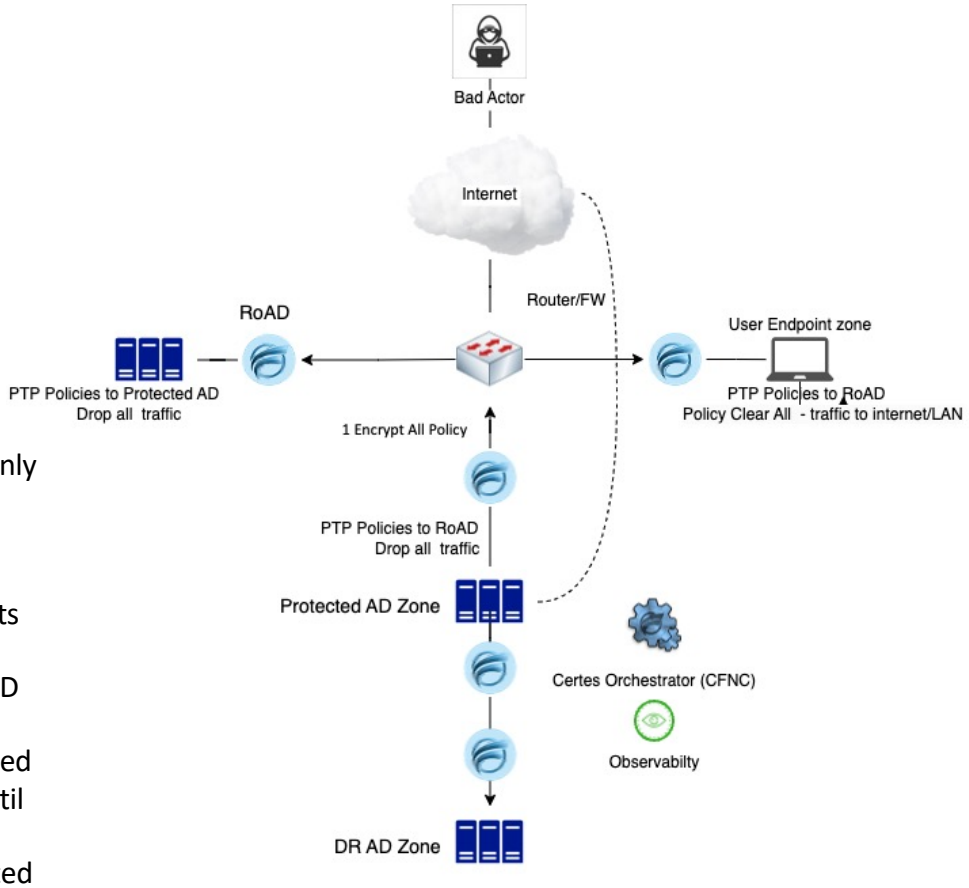
info@certes.ai

- Separate Data access from Network access
- Contain Malware blast radius
- Separate individual application data flows from one another
- Protect each data flow with a separate Quantum key.
- Make it impossible to identify sensitive / valuable data.
- Make it impossible to move laterally.
- Break stage 1,3,4,5 of the "Kill Chain"

- DPRM joins the network as a Layer2 device.
- No IP address on data plane ports
- No impact to traditional network security solutions
- Not discoverable
- FIPS 140-2 & CC EAL4+ certified.
- Stealth deployment.
- Break stage 1-2 of the "Kill Chain"

- Control the directional flow of data – DataDiode
- Stop Data flows by policy without changing Network Configuration - AirGap
- Define trusted and untrusted locations
- Prevent the exfiltration of data no matter what infrastructure has been attacked.
- Break stage 6-7 of the "Kill Chain"

Certes DPRM – Active Directory Protection deployment



- User authentication is with Readonly (RoAD) domain controller only
- Only authentications that passed through a CEP are allowed
- Legitimate authentication attempts not via a CEP are rejected
- Protected AD updates Readonly AD
- Protected AD updates DR
- Updates from Readonly are rejected
- Updates from DR are rejected (until Policy allows in a DR situation).
- ALL Data flowing from the Protected AD are via a CEP and will be Quantum protected.

Attack	Description	DPRM Response
Pass the hash	Stolen hash passwords used to impersonate valid user	Identity not used to define data access
Golden ticket	Compromise of KRBTGT account – allows them to create any level user account	Identity not used to define data access
Credential dumping	Extracting credentials using tools like 'Mimikatz' for offline decryption	DPRM prevents extraction of data to untrusted locations.
DCSync / DCShadow	Simulation of legitimate Domain Controller actions / tools allowing extraction of passwords and domain database for offline decryption.	DPRM not only identifies data and protects it, but also knows the direction in which data should be flowing. DPRM can prevent a DCSync attack by only allowing Domain Controller data to flow to approved locations preventing data extraction (Data Diode / Unidirectional control)
Lateral movement	Identifying sensitive data flows to enable movement across the network – "where's the Domain controller?"	By making individual data streams 'invisible' to one another through quantum cryptography, DPRM prevents an attacker from identifying what/where is valuable data.
Group Policy Objects	Attackers exploit poorly configured Group Policy Objects to apply malicious policies across the network, such as adding backdoors or disabling security settings.	The group policy management can be protected by DPRM ensuring that access and updates are only carried out from approved locations

The Cost of a Breach vs. the Cost of Prevention

The financial, operational, legal and reputational damage from a breach, particularly involving customer data, could easily reach millions in fines and lost trust. Based on a 15% to 20% probability of a breach occurring within the next 6 months, the importance of addressing these vulnerabilities becomes clear.

Investing in Certes not only helps protect sensitive data but also provides a clear financial benefit by minimizing these risks.