The Cloud Kill Chain

What is the Cloud Kill Chain?
The sequence of actions attackers put in place to gain unfettered access to virtualized infrastructure. For a highly virtualized organization, the cloud kill chain has the greatest potential to inflict damage while the attacker remains undetected.

The Nature of the Cloud: Today & Future

What is the Cloud Kill Chain?

Privileged Accounts and the Cloud Kill Chain

Cloud Adoption Statistics

Breaking the Cloud Kill Chain

HyTrust disrupts the cloud kill chain in three phases:

1/2 of worldwide software, server and storage growth will come from public IT cloud services by 2018 (IDC)

Existing management tools do not offer these capabilities.

1/2 of worldwide software, server and storage growth will come from public IT cloud services by 2018 (IDC)

Existing management tools do not offer these capabilities.

Two-factor authentication

Password vaulting

Stronger Authentication

Two-person authorization

Granular auditing and alerts

Control and Alert

Two-person authorization

Granular auditing and alerts

Control and Alert

Delivery

Exploitation

Exfiltration

Recon

Privileged malware

Enable or bypass controls

Delete evidence of presence

Command and Control

Establish communication channels outside the organization.

Snapshot virtual machines, data or cause catastrophic failure by deleting or suspending virtual machines.

Actions/Exfiltration

Research, identification and selection of targets with the objective of gaining access to entire set of virtualized resources (virtual machines, network segments, data stores).

Delivery

Deliver malware to one or more hosts through advanced threats like email attachments, spear phishing, back-doored IT equipment.

Exploitation

Install supporting elements and capture administrative credentials for virtualized infrastructure, granting the attacker substantially broader controls.

Command and Control

Leverages advanced network and endpoint security, log management and monitoring solutions.

Ensures all systems, applications and security software are patched and up-to-date.

HyTrust disrupts the cloud kill chain in three phases:

1. Recon
   - Research, identification and selection of targets with the objective of gaining access to entire set of virtualized resources (virtual machines, network segments, data stores).

2. Delivery
   - Deliver malware to one or more hosts through advanced threats like email attachments, spear phishing, back-doored IT equipment.

3. Exploitation
   - Install supporting elements and capture administrative credentials for virtualized infrastructure, granting the attacker substantially broader controls.

4. Command and Control
   - Establish communication channels outside the organization.

   - Snapshot virtual machines, data or cause catastrophic failure by deleting or suspending virtual machines.

5. Actions/Exfiltration
   - Research, identification and selection of targets with the objective of gaining access to entire set of virtualized resources (virtual machines, network segments, data stores).

To break the Cloud Kill Chain:

- Identify and eliminate weak points in security protocols.
- Implement strong authentication methods.
- Regularly update security software and systems.
- Use advanced monitoring and log management tools.

For more information about how HyTrust can help secure your private, hybrid or public cloud infrastructure, visit http://hytrust.com/products/why-hytrust or call 1-650-681-8100.