

Common Sub Trees for NESCOR Failure Scenarios

Version 1.6



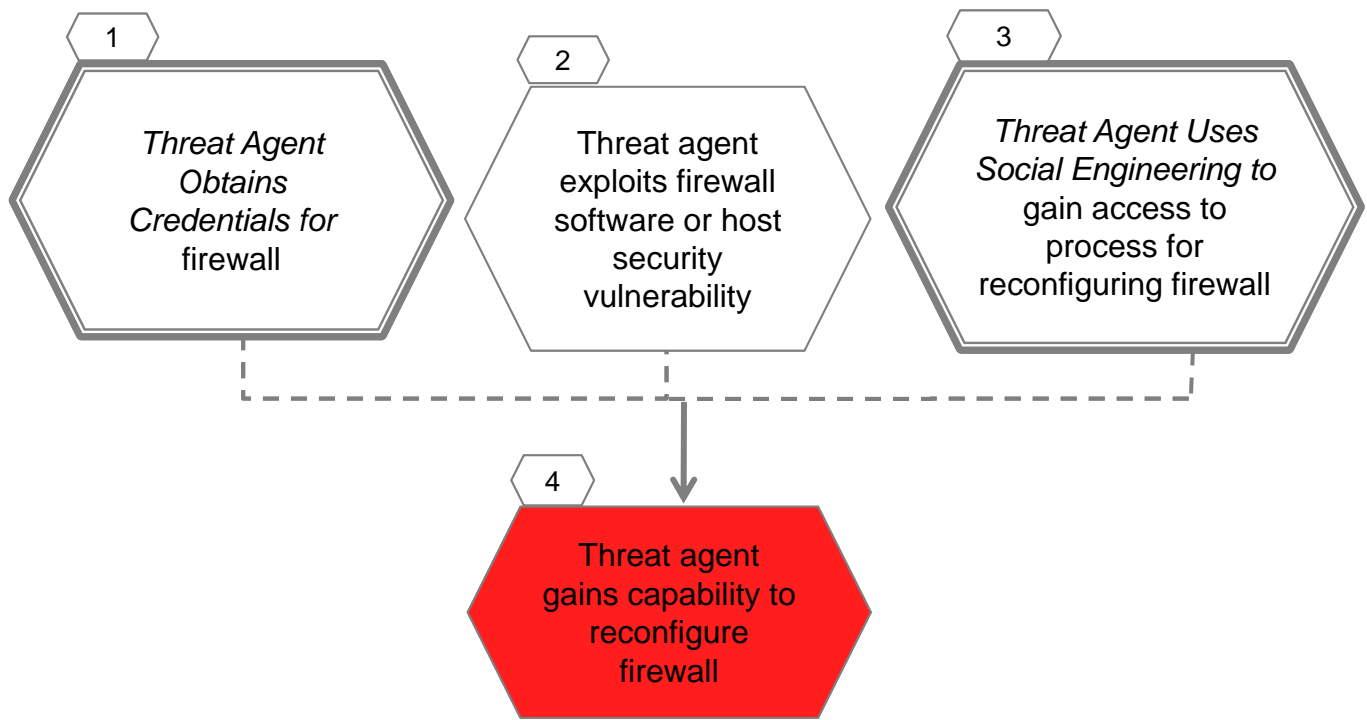
May 2015

Common Sub Trees

- Threat Agent Gains Capability to Reconfigure <firewall>
- Threat Agent Blocks Wireless Communication Channel Connecting <x and y>
- Authorized Employee Brings Malware into <system or network>
- Threat Agent Obtains Credentials for <system or function>
- Threat Agent Uses Social Engineering to <desired outcome>
- Threat Agent Exploits Firewall Gap in <specific firewall>
- Threat Agent Exfiltrates <data>
- Threat Agent Gains Access to <network>

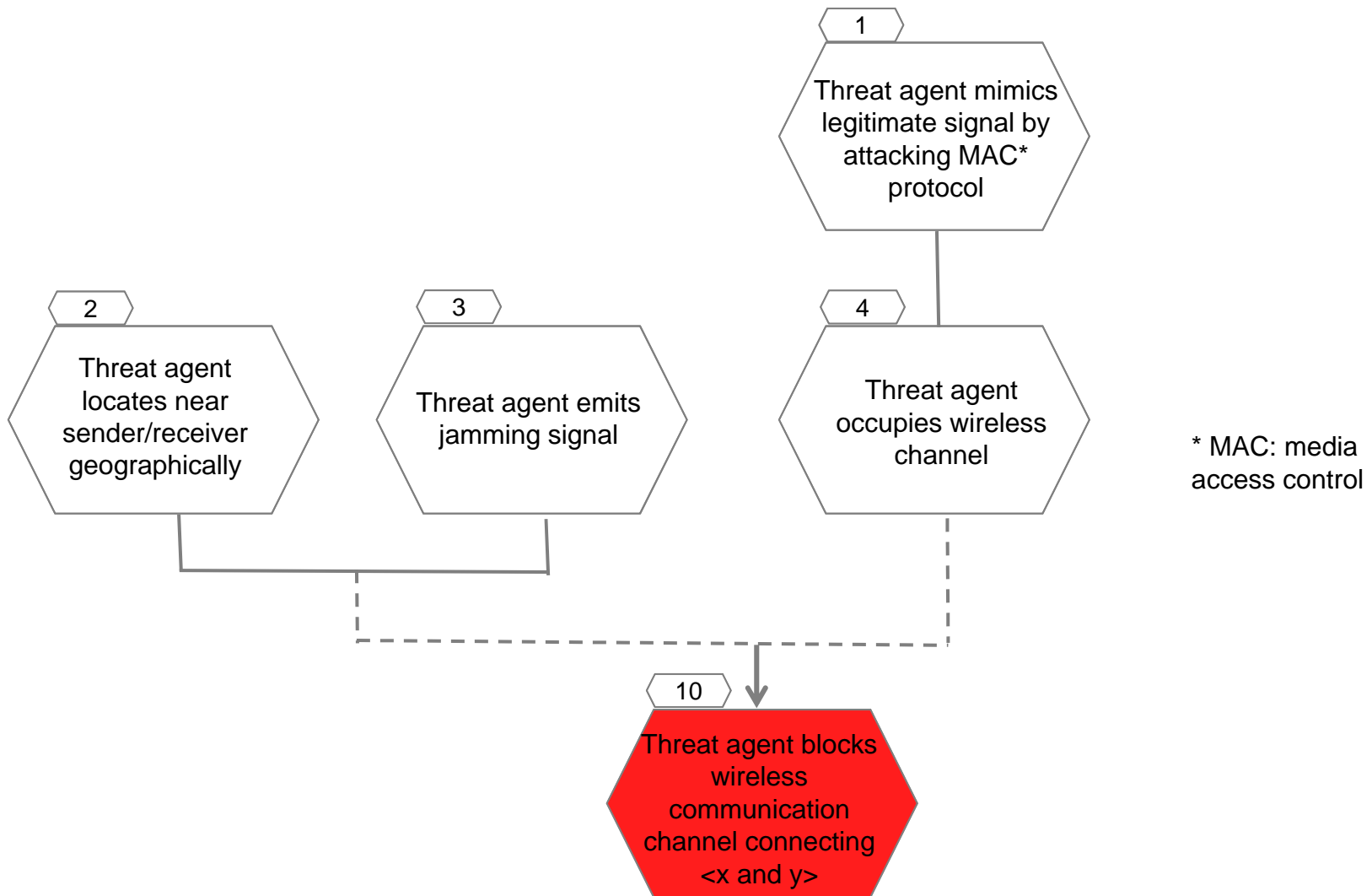
Common Tree: Threat Agent Gains Capability to Reconfigure <firewall>

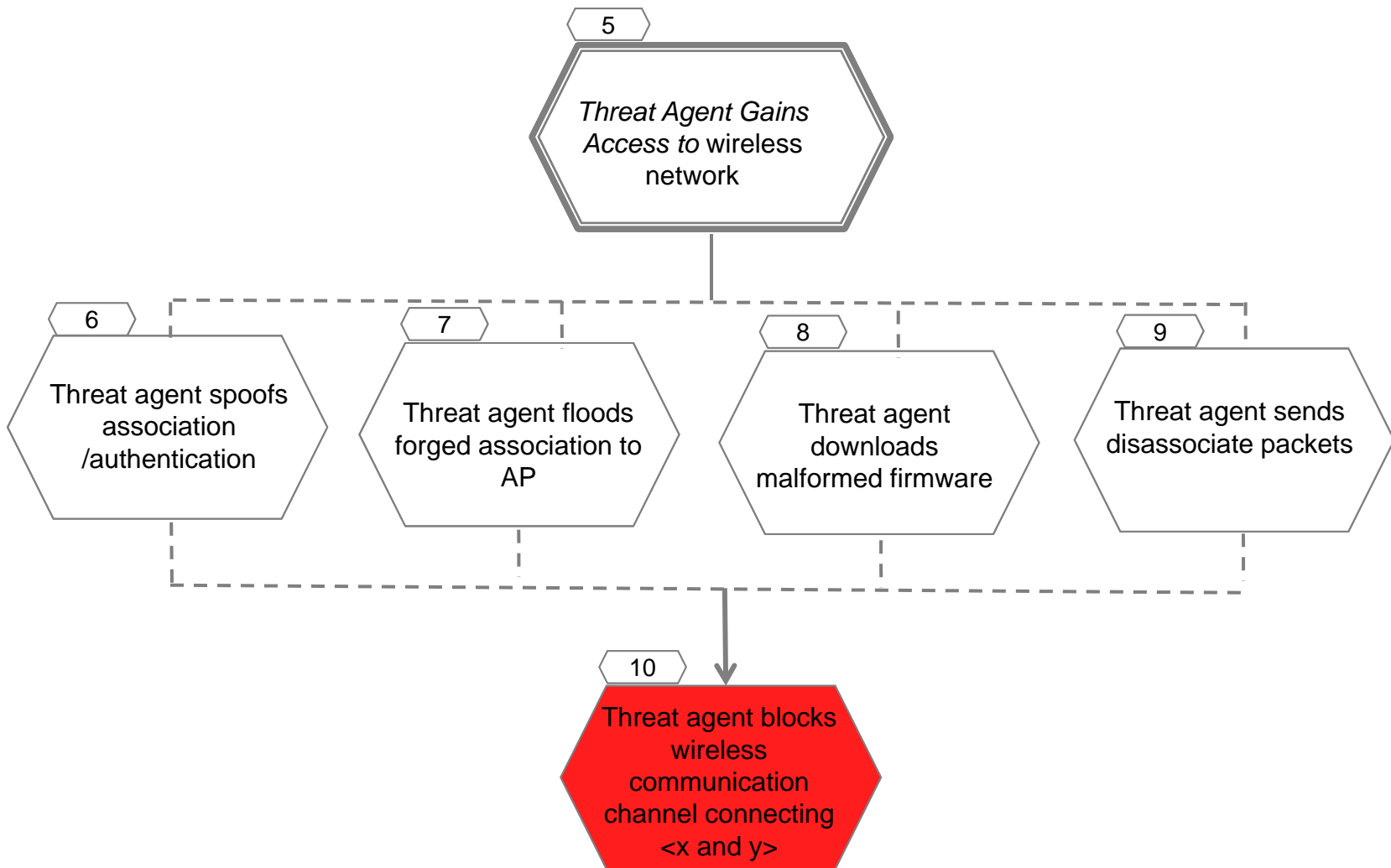
- **Description:** A threat agent gains the capability to change firewall rules on a specific firewall to permit types of traffic to flow through the firewall that will enable future attacks.



Common Tree: Threat Agent Blocks Wireless Communication Channel Connecting <x and y>

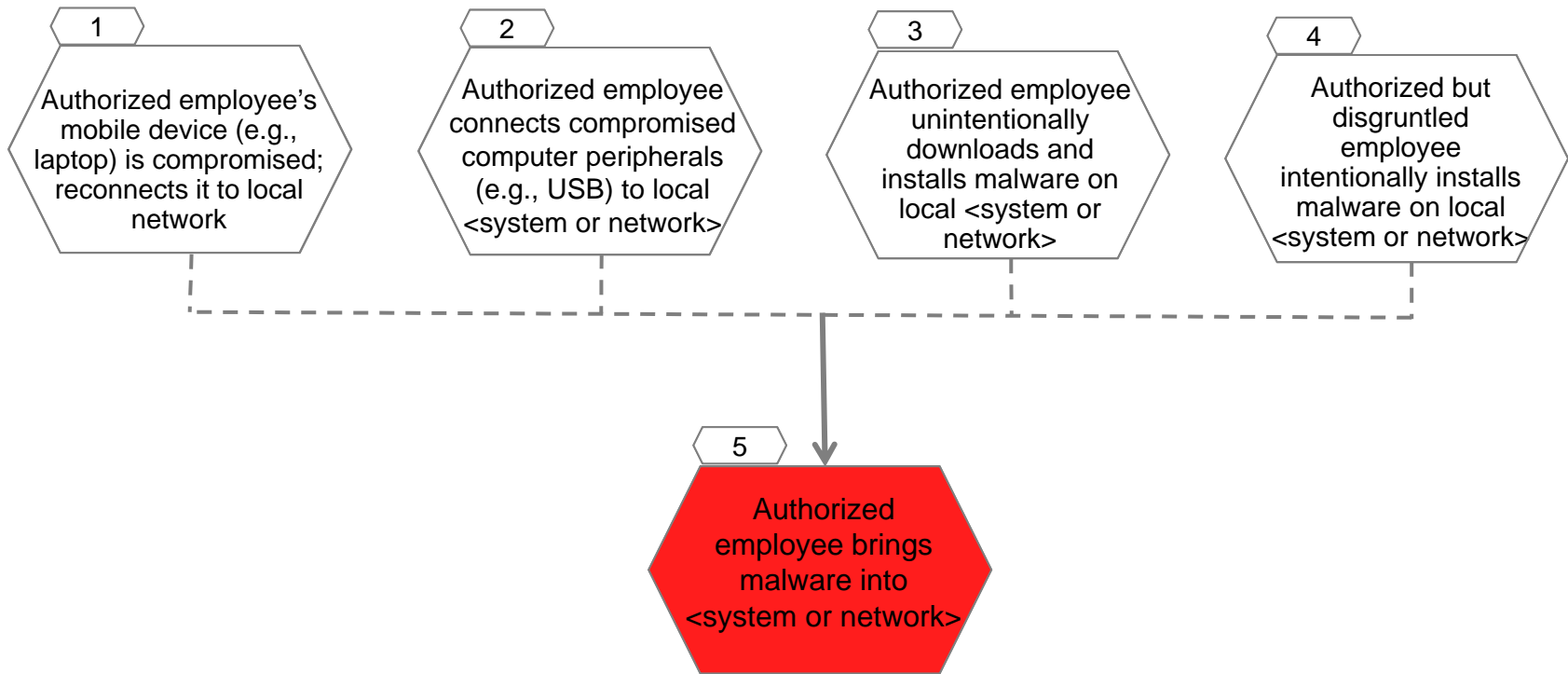
- **Description:** The threat agent stops the flow of messages on a wireless communication channel connecting two entities, or slows it down to a point that it is essentially stopped.





Common Tree: Authorized Employee Brings Malware into <system or network>

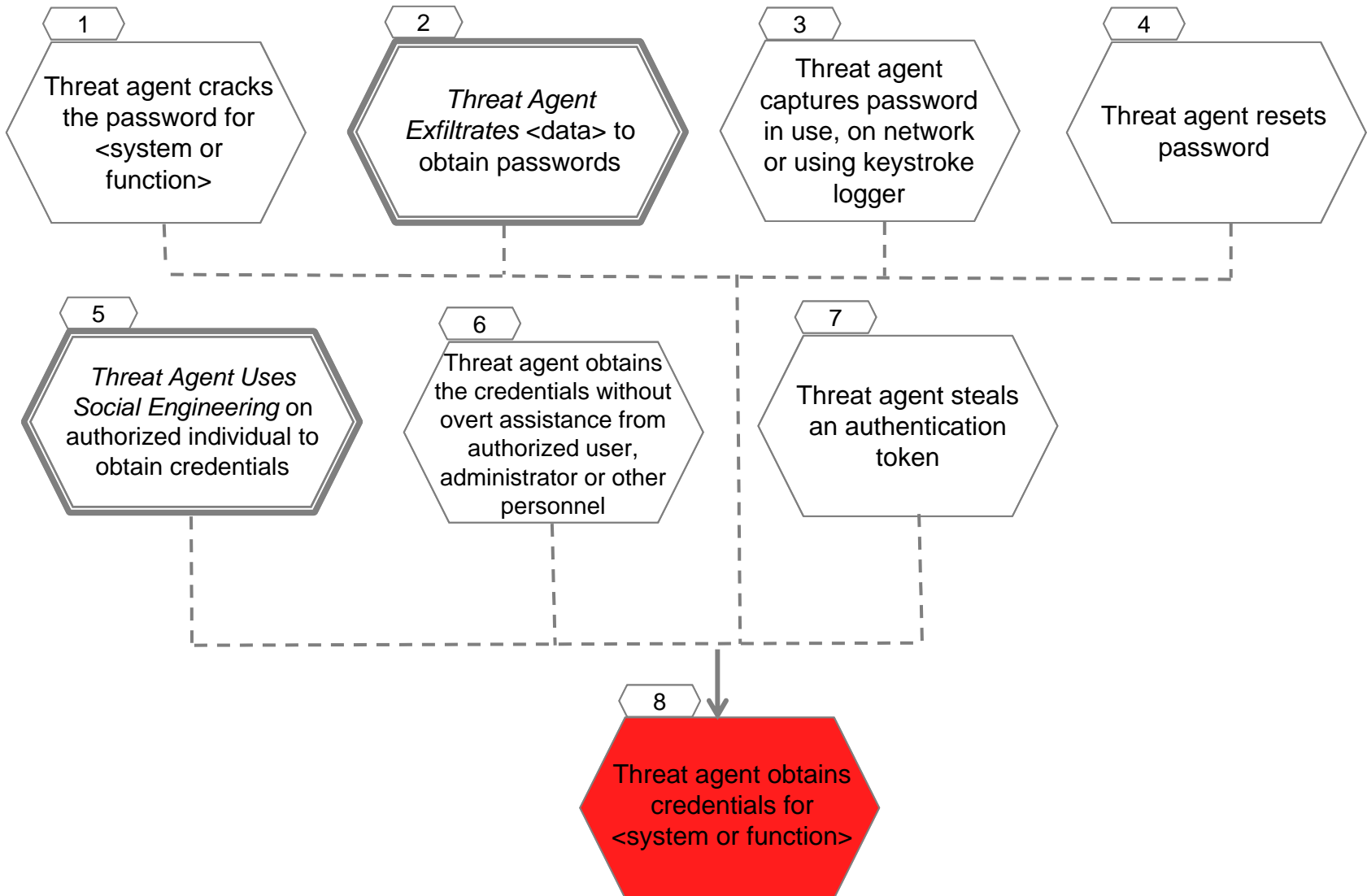
- **Description:** An authorized employee uses the IT infrastructure to perform any action that results in the introduction of a particular piece of malware onto a specific network or a system.



Common Tree: Threat Agent Obtains Credentials for <system or function>

■ Description

- A threat agent may gain credentials for a system, or credentials that provide privileges to perform specific functions, in a number of ways. This includes finding them, stealing them, guessing them, or changing them. The threat agent may use social engineering techniques to carry out these methods. Each technology and implementation used for credentials is resistant to some methods and susceptible to others.

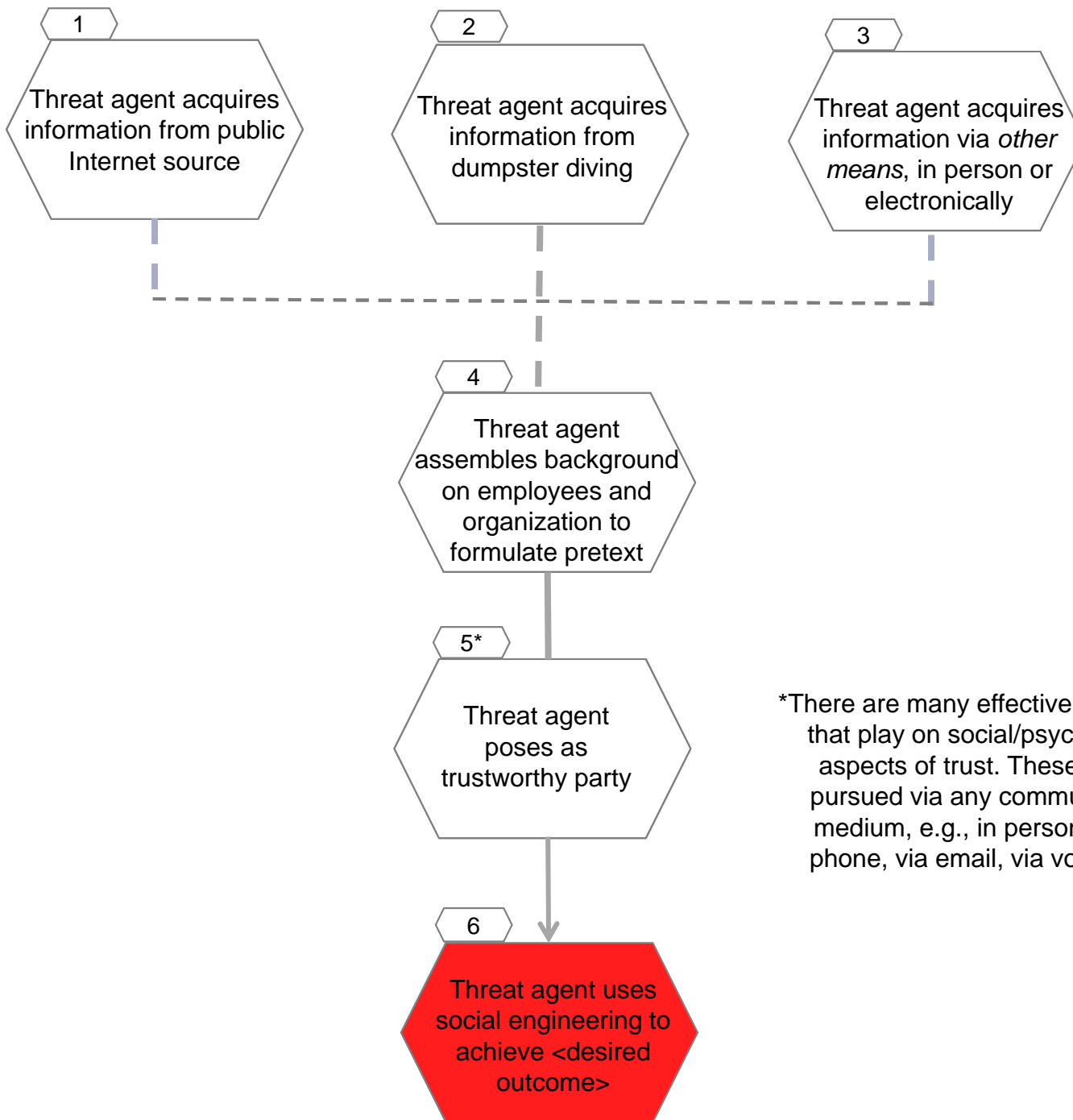


Common Tree: Threat Agent Uses Social Engineering to <desired outcome>

- **Description:** A threat agent uses techniques of social engineering to persuade a victim to perform a desired action that results in an outcome that benefits the threat agent. Common examples of actions are to disclose particular information or to install/execute software that collects information or harms the victim's IT environment.

- **Notes**

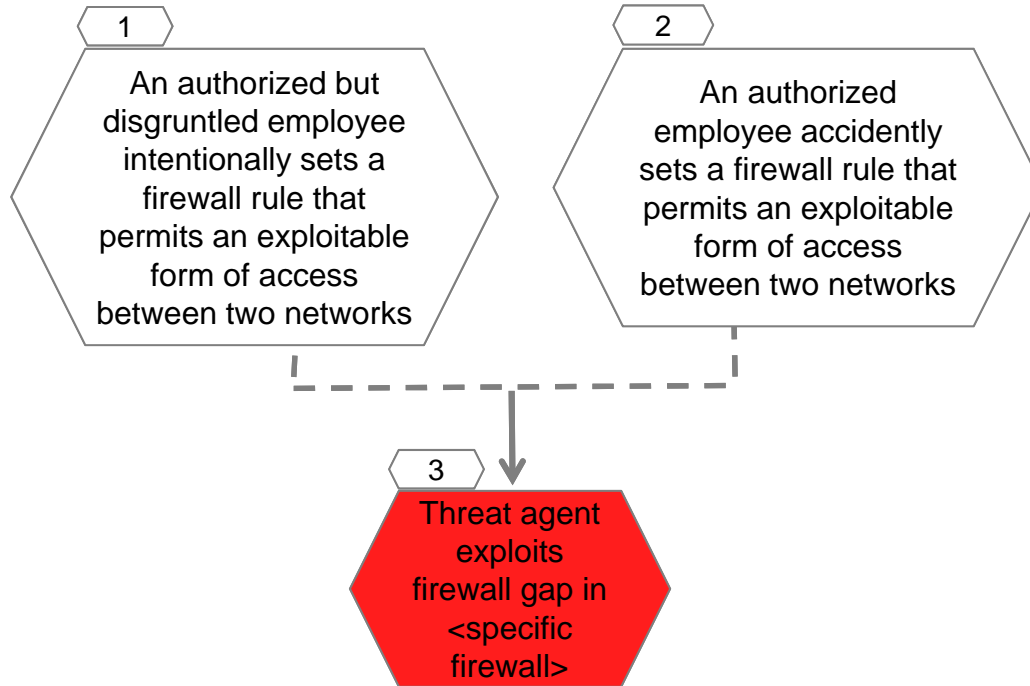
- The attack tree provides an overview of the use of social engineering, there are many varieties
- More details and common examples may be found at:
http://www.social-engineer.org/framework/Social_Engineering_Framework



*There are many effective techniques that play on social/psychological aspects of trust. These can be pursued via any communication medium, e.g., in person, on the phone, via email, via voice mail.

Common Tree: Threat Agent Exploits Firewall Gap in <specific firewall>

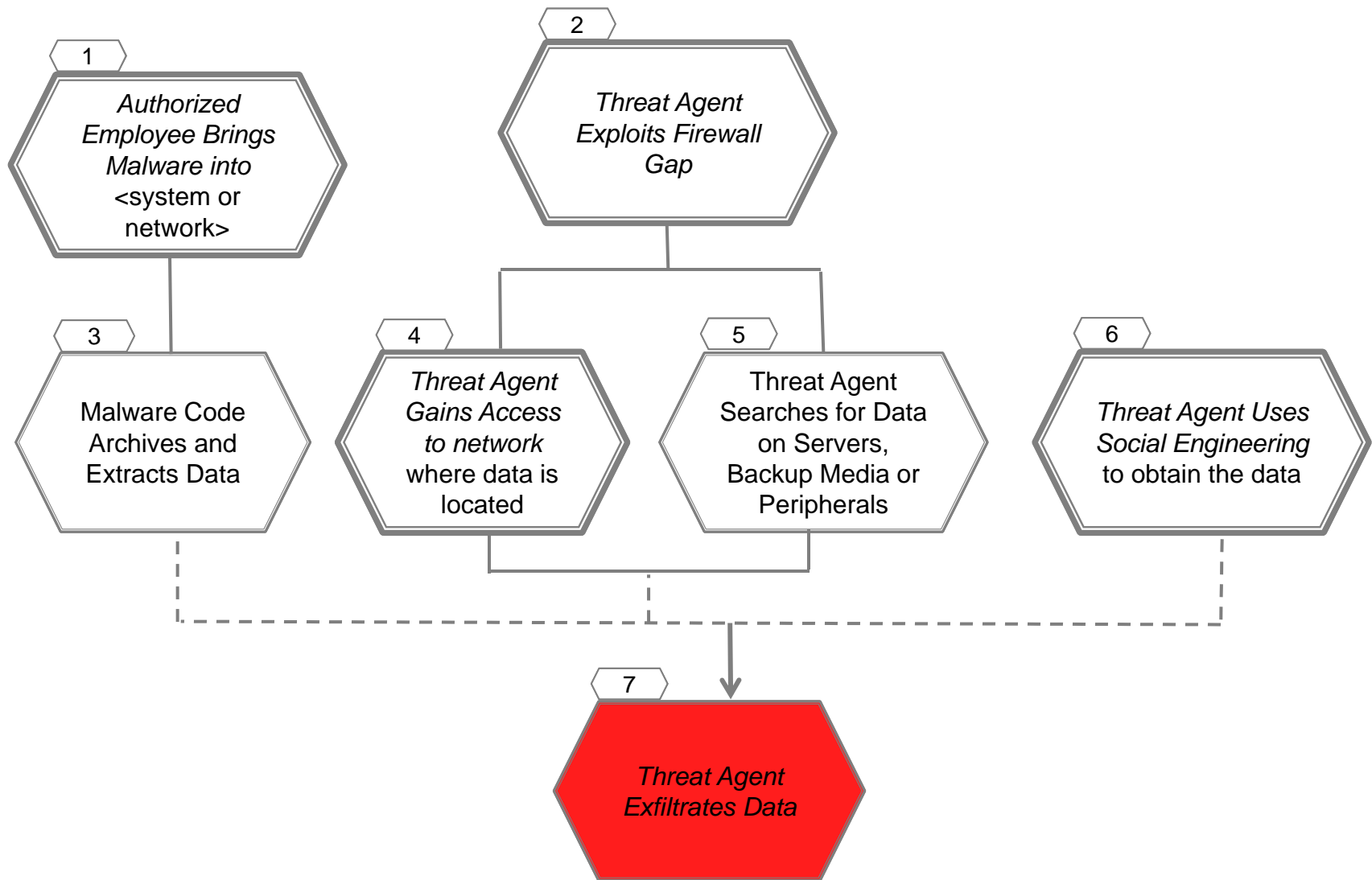
- **Description:** An authorized employee either accidentally or intentionally sets a firewall rule that allows an unnecessary and exploitable form of access to a network from another network.



Common Tree: Threat Agent Exfiltrates <Data>

■ Description

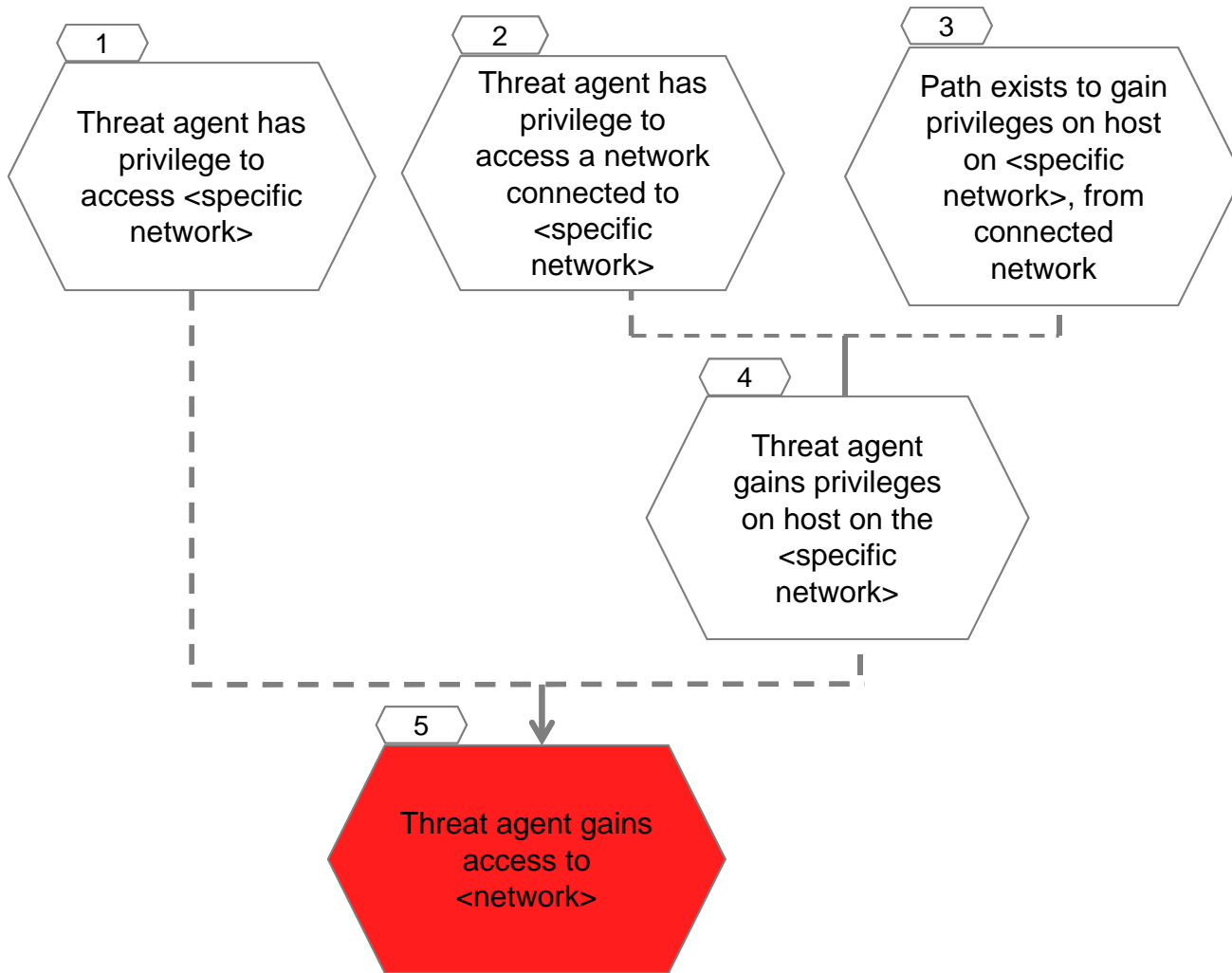
- A threat agent may use direct or indirect methods to obtain a copy of a file or data, including a direct break-in to the host holding the file, finding the data on back up media, scanning peripherals such as printers, and use of social engineering to influence a victim to give them the data.



Common Tree: Threat Agent Gains Access to <network>

■ Description

- A threat agent becomes capable of sending traffic within a network and attempting to communicate with its resident hosts.





Together...Shaping the Future of Electricity