Common Sub Trees for NESCOR Failure Scenarios

Version 1.5

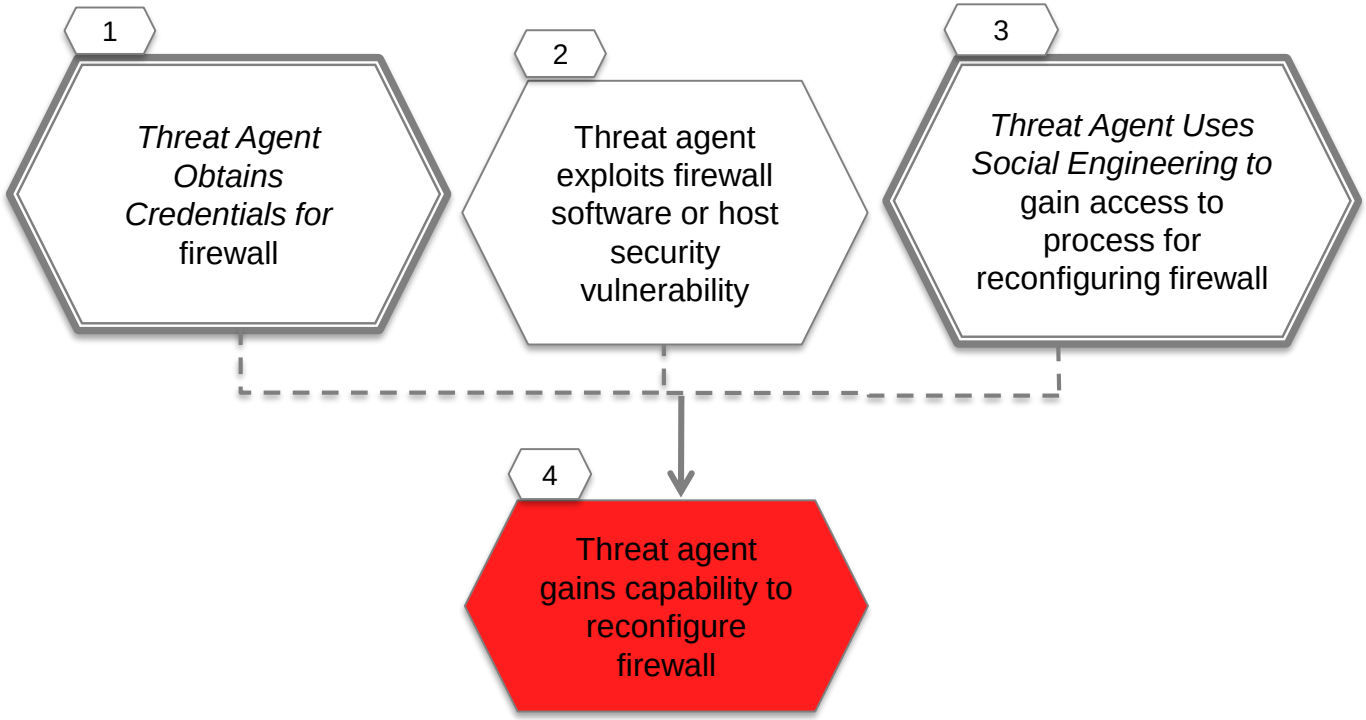
May 2015

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>

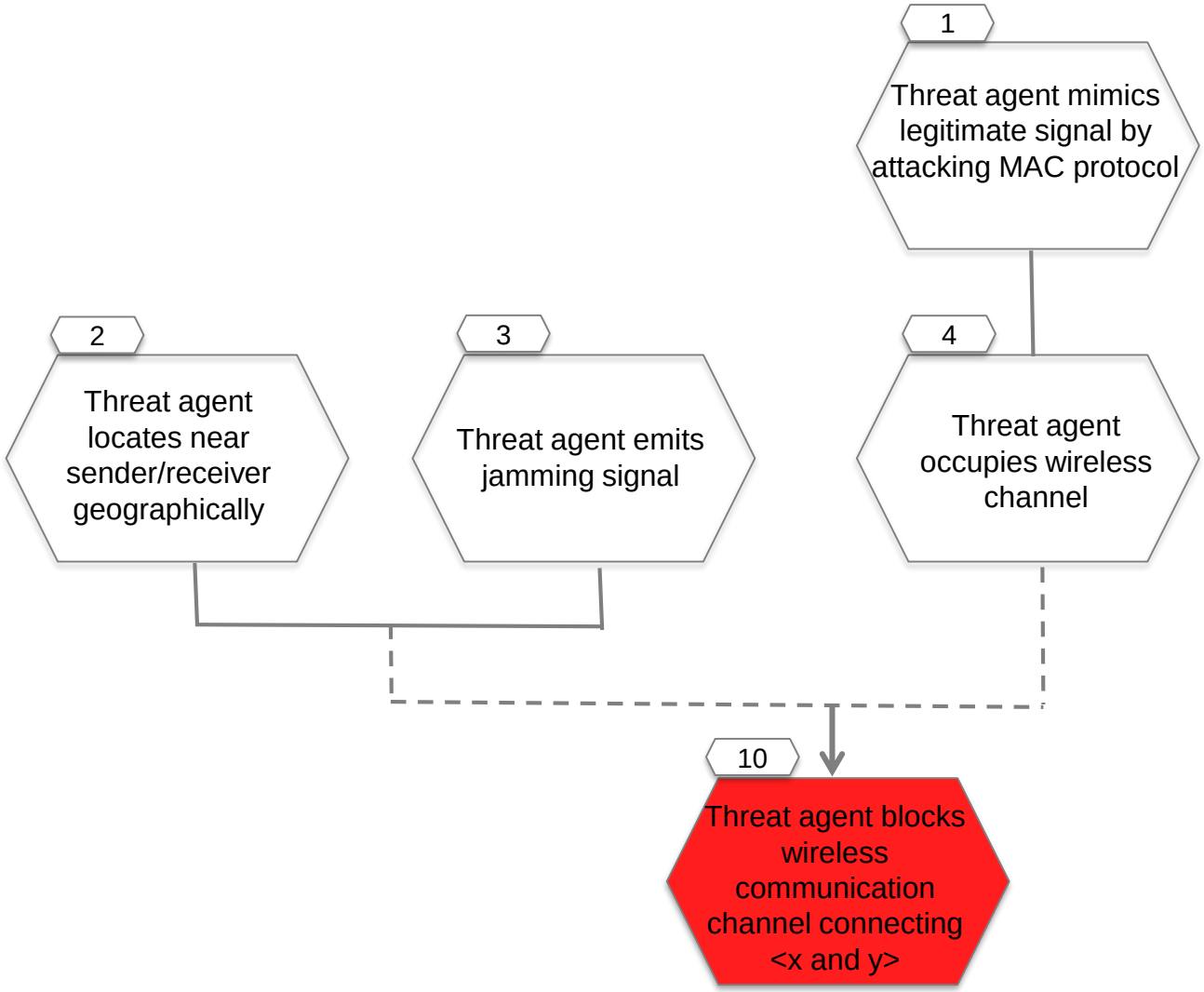
Common Tree: Threat Agent Gains Capability to Reconfigure <firewall>

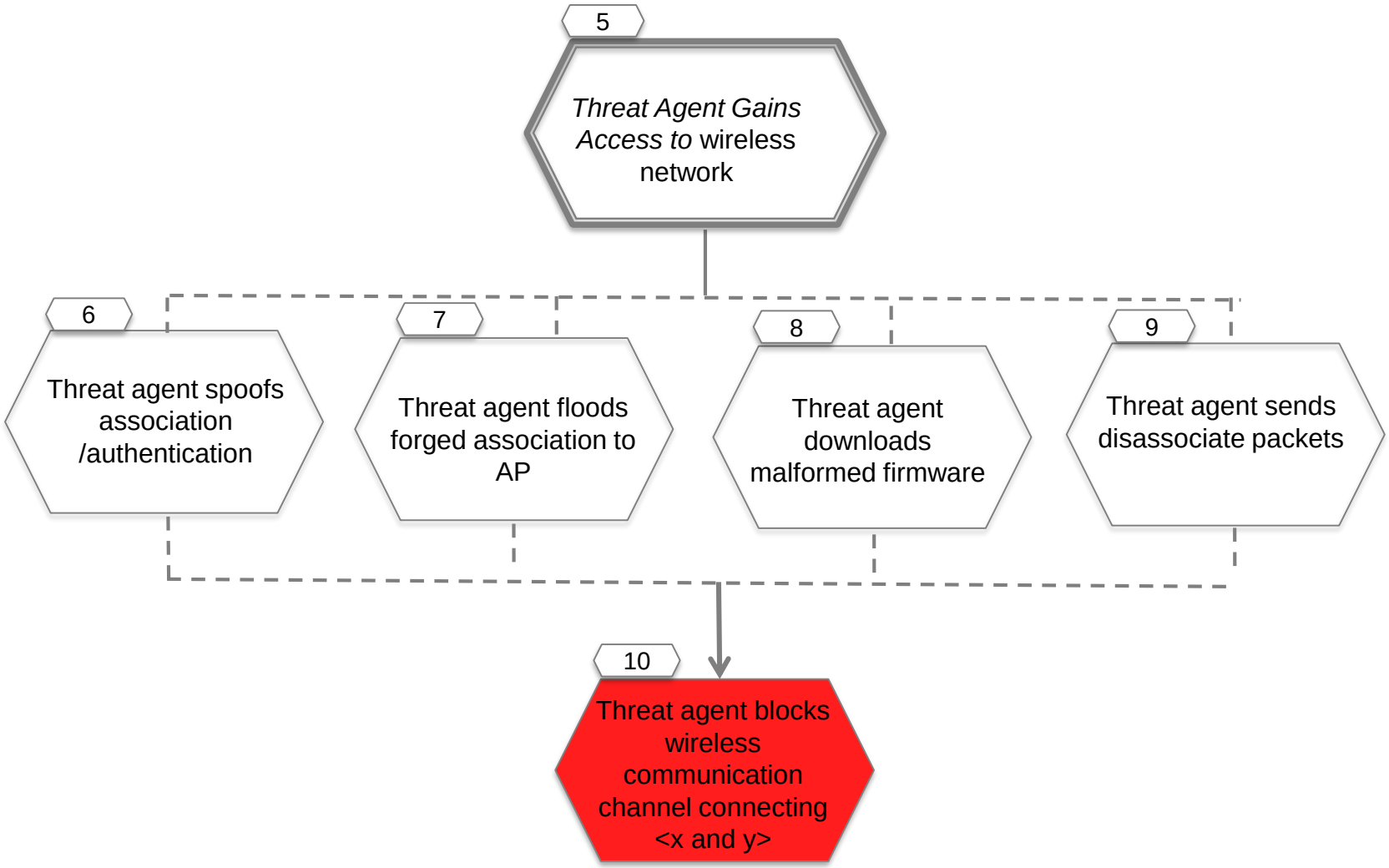
- **Description:** A threat agent gains the capability to change firewall rules on a specific firewall to permit types of traffic to flow through the firewall that will enable future attacks.


1
Threat Agent Obtains Credentials for firewall
2
Threat agent exploits firewall software or host security vulnerability
3
Threat Agent Uses Social Engineering to gain access to process for reconfiguring firewall
4
Threat agent gains capability to reconfigure firewall

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.

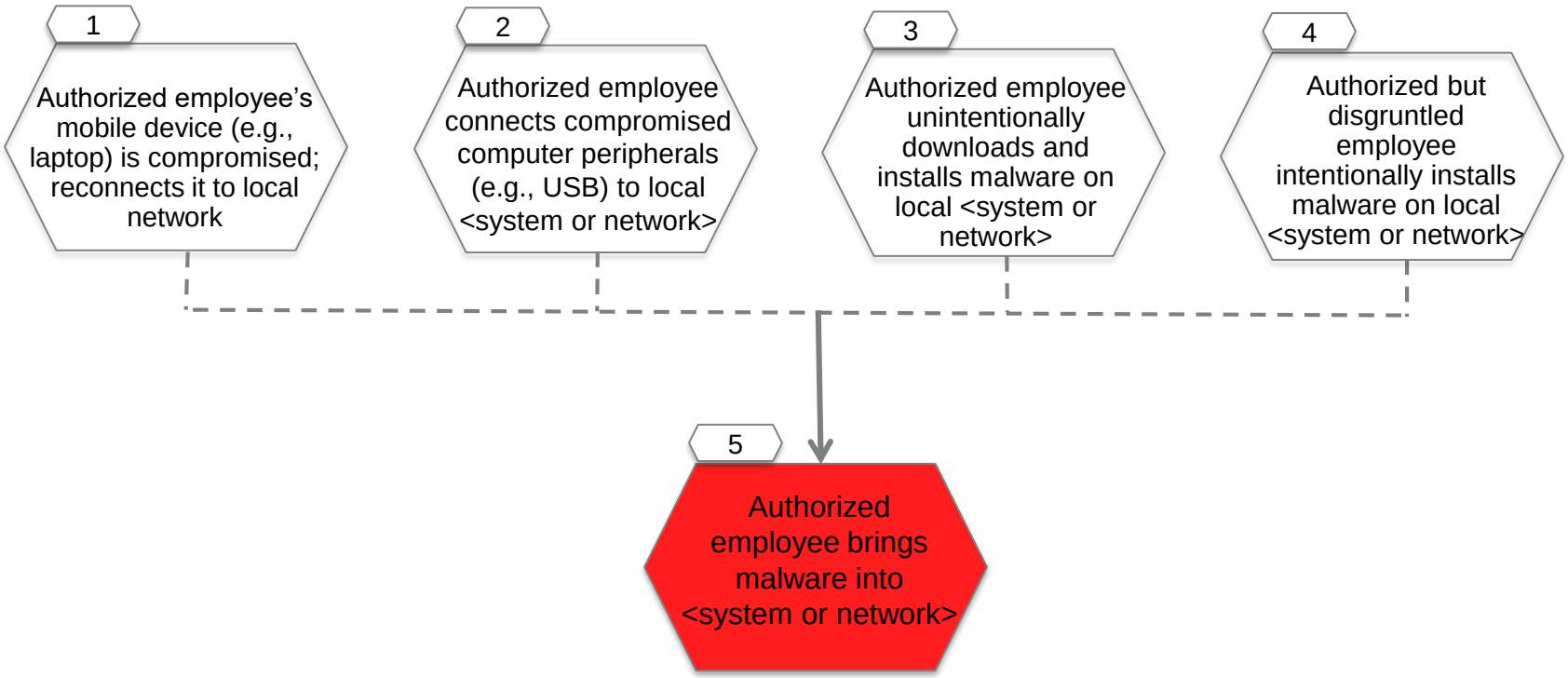

1
Threat agent mimics legitimate signal by attacking MAC protocol
2
Threat agent locates near sender/receiver geographically
3
Threat agent emits jamming signal
4
Threat agent occupies wireless channel
10
Threat agent blocks wireless communication channel connecting <x and y>


5
Threat Agent Gains Access to wireless network
6
Threat agent spoofs association /authentication
7
Threat agent floods forged association to AP
8
Threat agent downloads malformed firmware
9
Threat agent sends disassociate packets
10
Threat agent blocks wireless communication channel connecting <x and y>

(2/2)

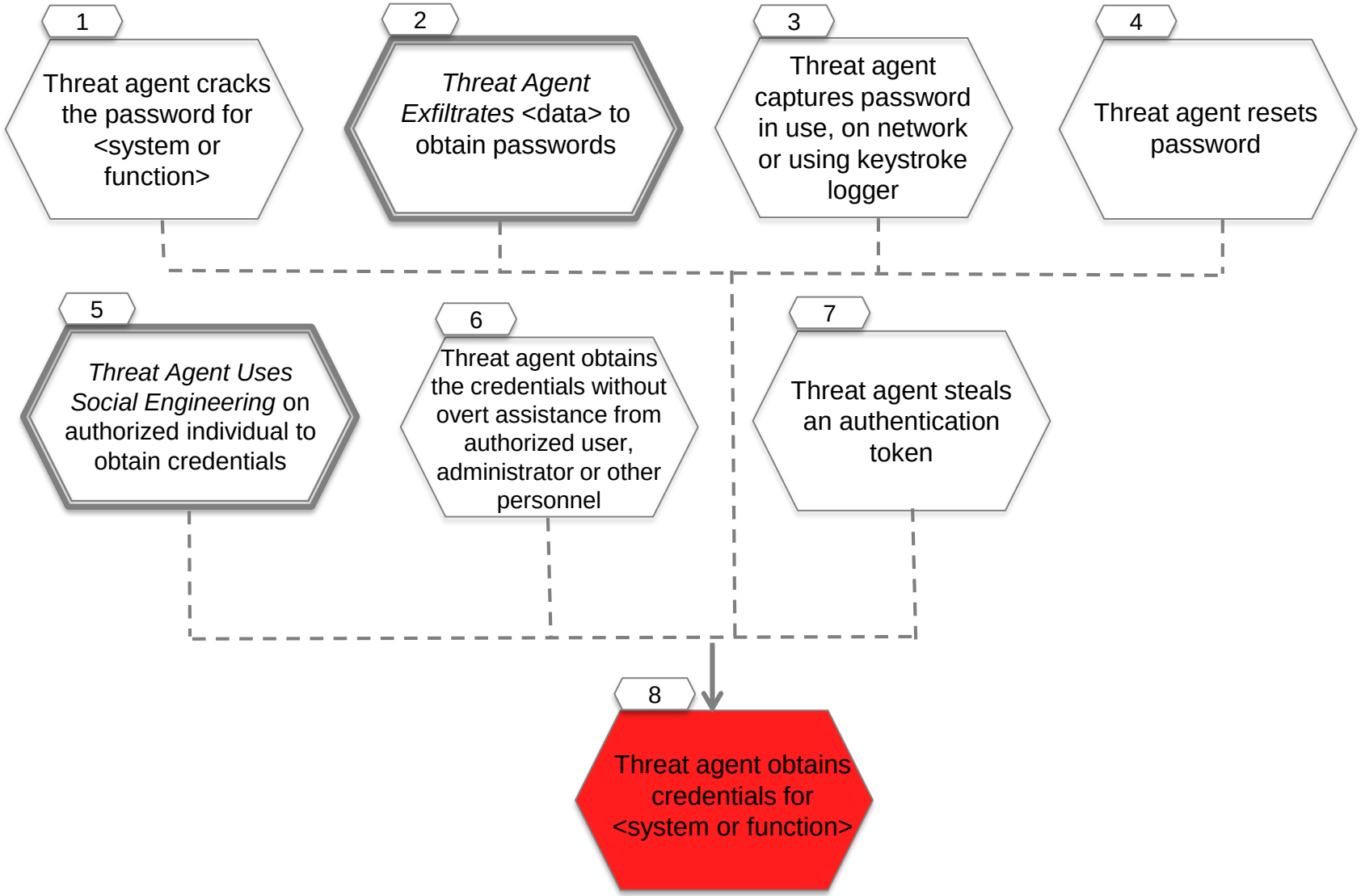
Common Tree: Authorized Employee Brings Malware into <system or network>

- **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.


1
Authorized employee's mobile device (e.g., laptop) is compromised; reconnects it to local network
2
Authorized employee connects compromised computer peripherals (e.g., USB) to local <system or network>
3
Authorized employee unintentionally downloads and installs malware on local <system or network>
4
Authorized but disgruntled employee intentionally installs malware on local <system or network>
5
Authorized employee brings malware into <system or network>

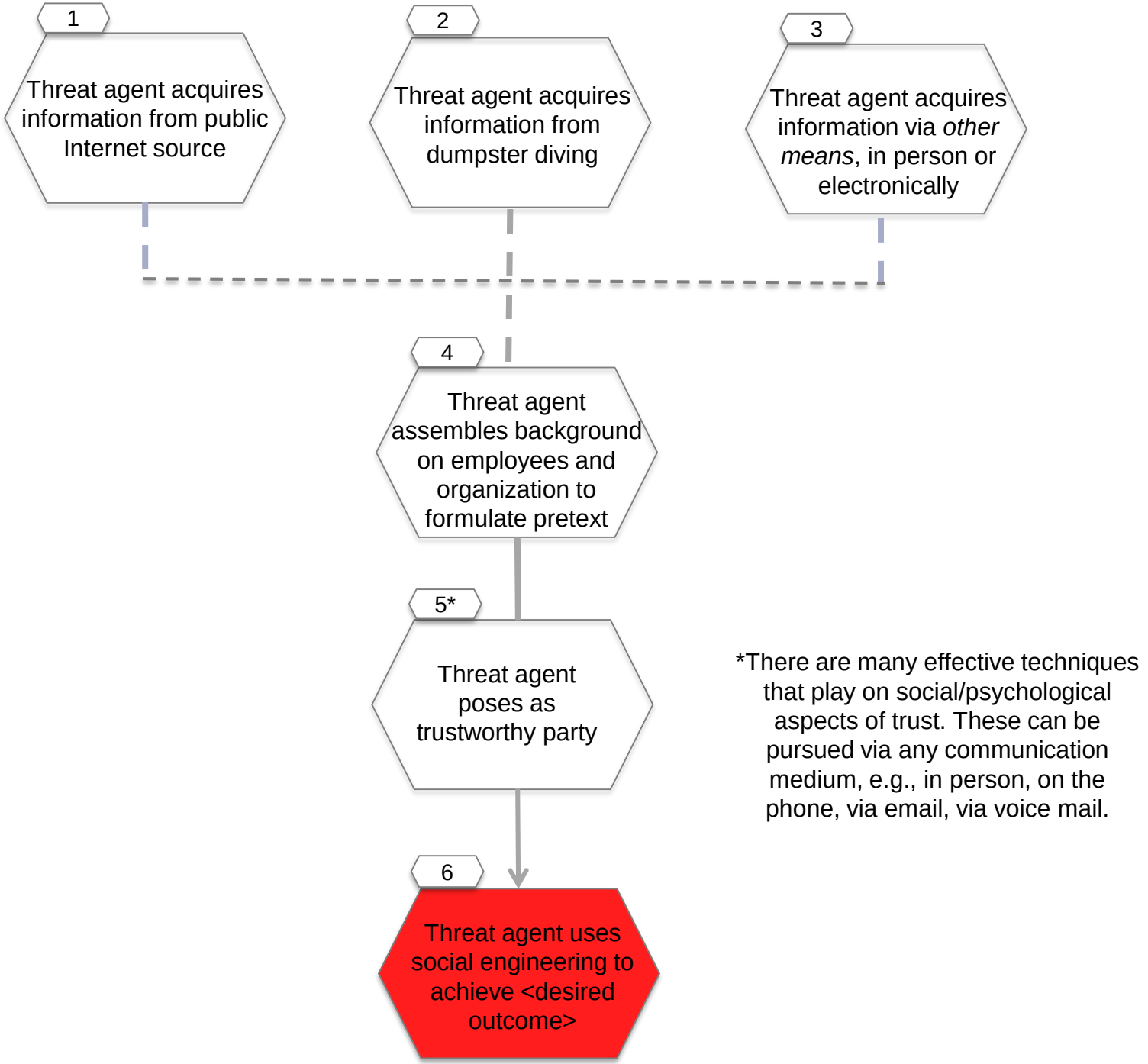
Common Tree: Threat Agent Obtains Credentials for <system or function>

- **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.


1
Threat agent cracks the password for <system or function>
2
Threat Agent Exfiltrates <data> to obtain passwords
3
Threat agent captures password in use, on network or using keystroke logger
4
Threat agent resets password
5
Threat Agent Uses Social Engineering on authorized individual to obtain credentials
6
Threat agent obtains the credentials without overt assistance from authorized user, administrator or other personnel
7
Threat agent steals an authentication token
8
Threat agent obtains credentials for <system or function>

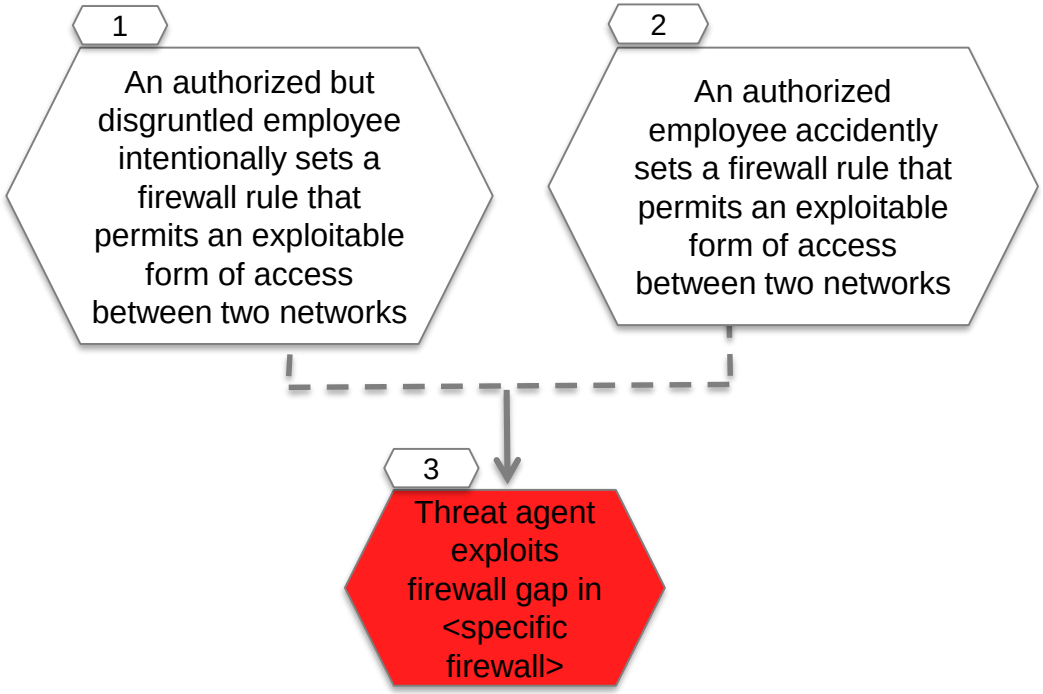
Common Tree: Threat Agent Uses Social Engineering to <desired outcome>

- **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


1
Threat agent acquires information from public Internet source
2
Threat agent acquires information from dumpster diving
3
Threat agent acquires information via *other means*, in person or electronically
4
Threat agent assembles background on employees and organization to formulate pretext
5*
Threat agent poses as trustworthy party
6
Threat agent uses social engineering to achieve <desired outcome>
*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.

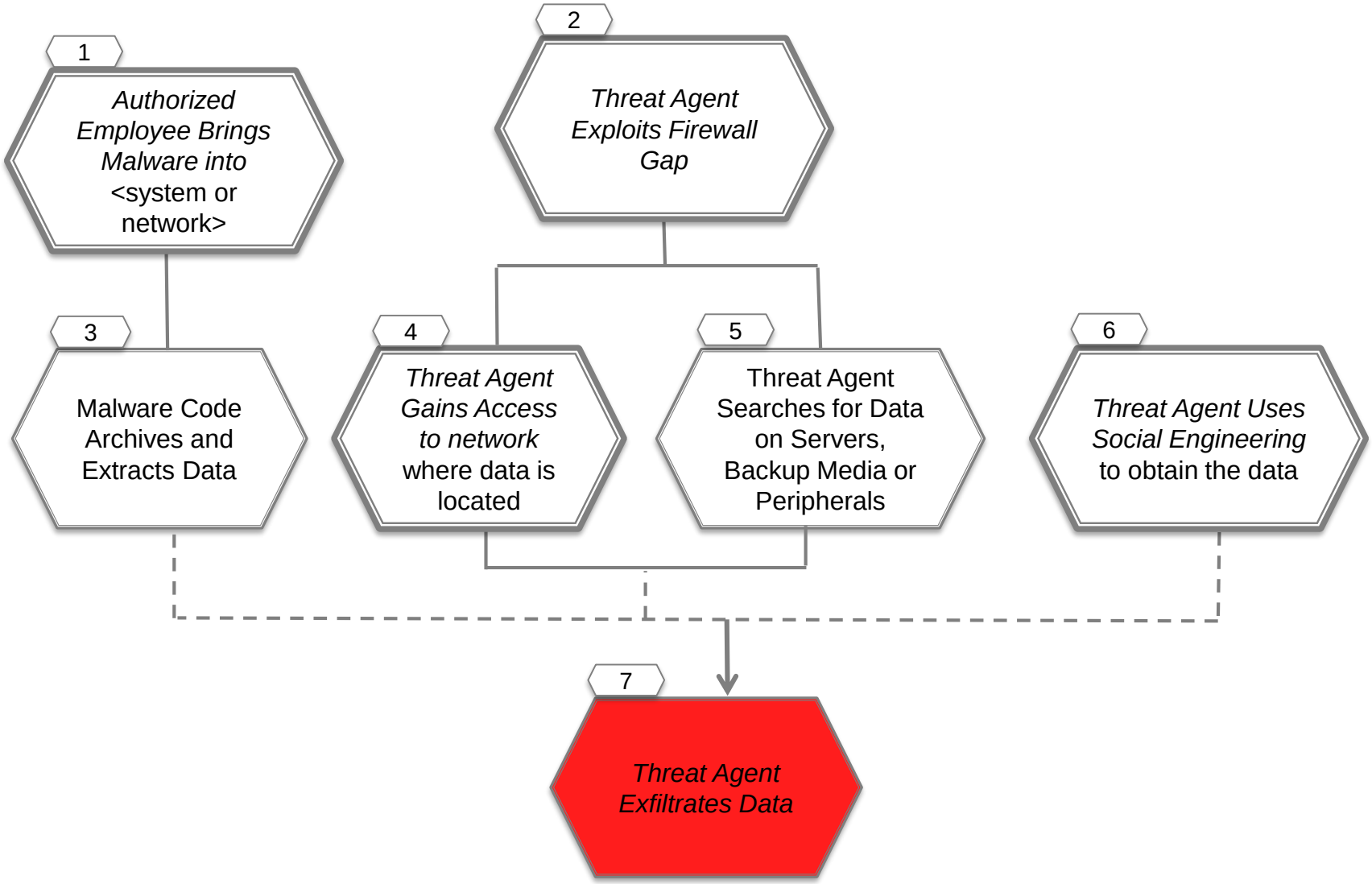
Common Tree: Threat Agent Exploits Firewall Gap in <specific firewall>

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


1
An authorized but disgruntled employee intentionally sets a firewall rule that permits an exploitable form of access between two networks
2
An authorized employee accidently sets a firewall rule that permits an exploitable form of access between two networks
3
Threat agent exploits firewall gap in <specific firewall>

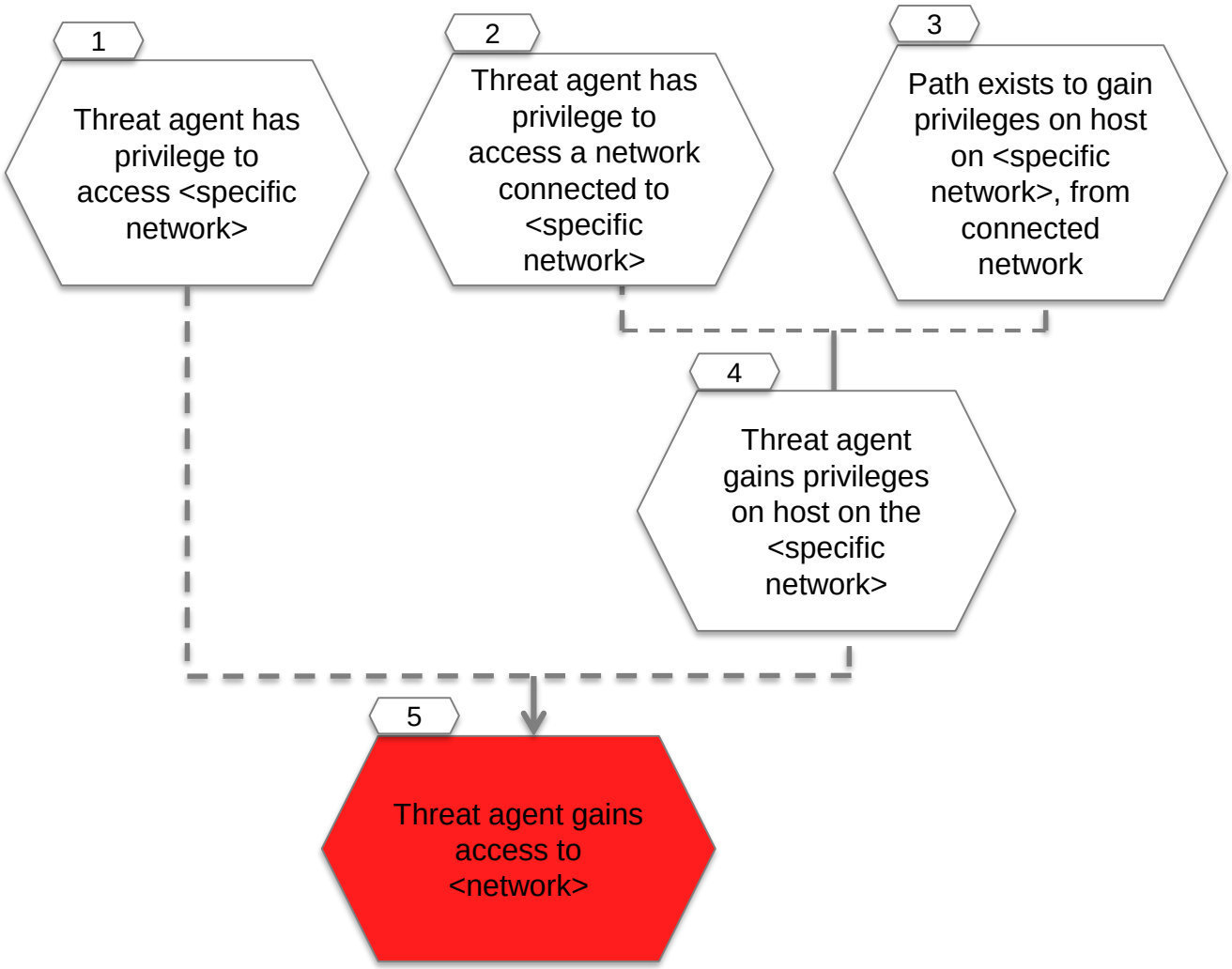
Common Tree: Threat Agent Exfiltrates <Data>

- **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.


1
Authorized Employee Brings Malware into <system or network>
2
Threat Agent Exploits Firewall Gap
3
Malware Code Archives and Extracts Data
4
Threat Agent Gains Access to network where data is located
5
Threat Agent Searches for Data on Servers, Backup Media or Peripherals
6
Threat Agent Uses Social Engineering to obtain the data
7
Threat Agent Exfiltrates 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.
- **Note:** This draft tree currently expresses the high level concept of "bridging" sequentially between adjacent networks. Information should be added in future drafts related to:
  - Mitigations for detecting and preventing network reconnaissance
  - Specific differences in gaining access to networks that use various protocols and technologies


1
Threat agent has privilege to access <specific network>
2
Threat agent has privilege to access a network connected to <specific network>
3
Path exists to gain privileges on host on <specific network>, from connected network
4
Threat agent gains privileges on host on the <specific network>
5
Threat agent gains access to <network>

Together…Shaping the Future of Electricity