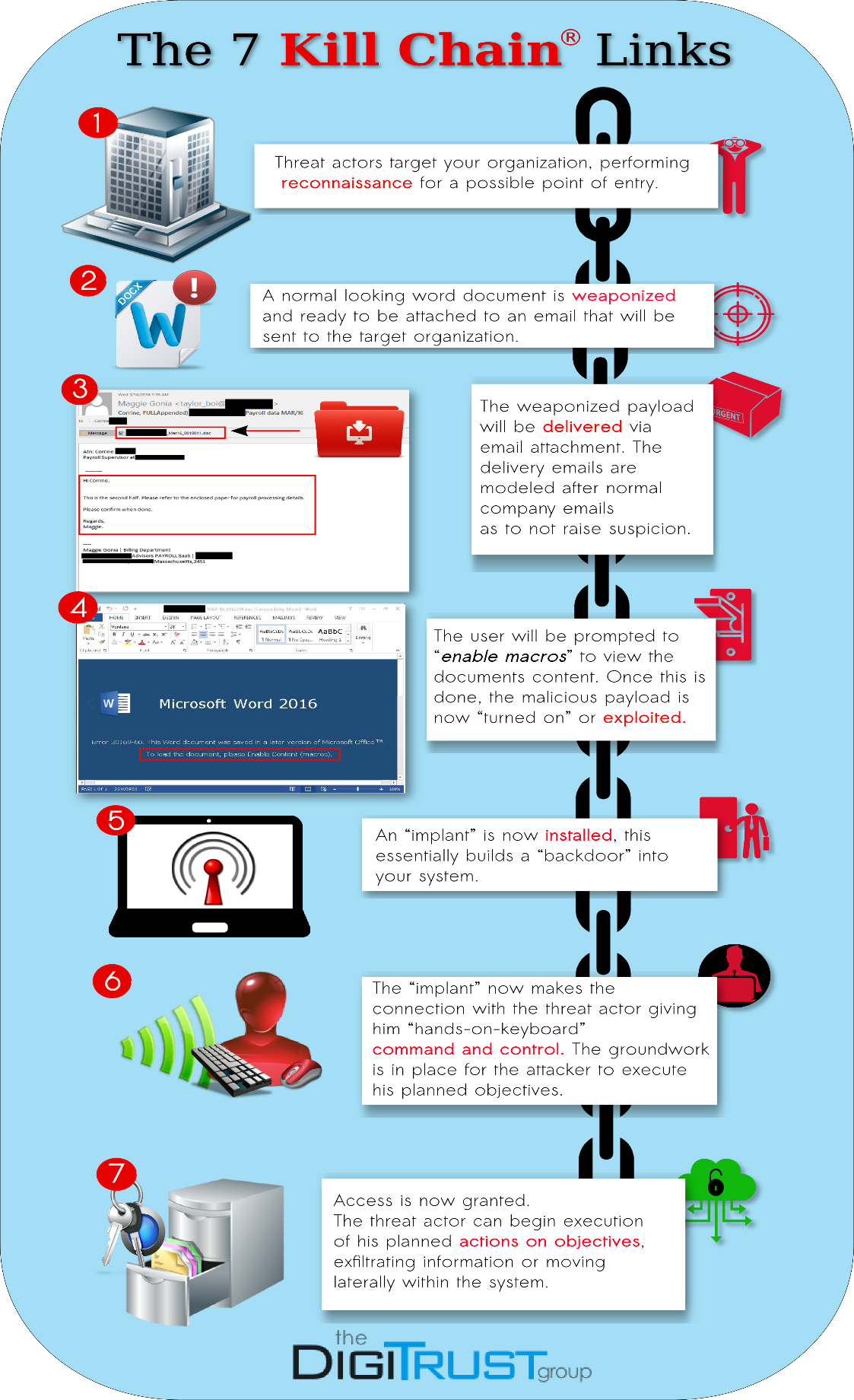
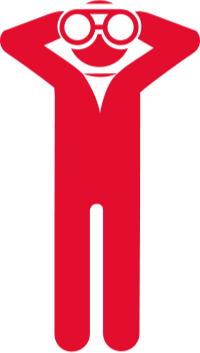
**Cyber Kill Chain model:**



**1. Reconnaissance: Understanding the Target**The threat actor begins with reconnaissance. The threat actor will often crawl websites gathering information such as email addresses, social media connections, or specific information on your organization’s technologies or processes.  
  
**The goal for the attacker is to gather any valuable information that will offer an access point to the target organization.**

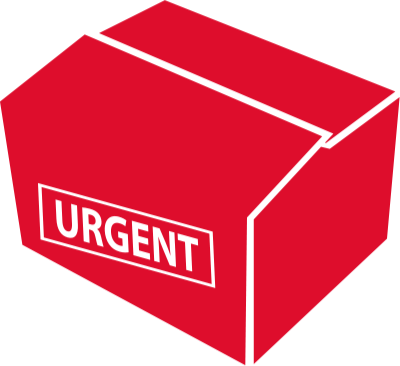


**2. Weaponization: Arming the Payload**What exactly does this malicious threat actor use to gain access? The answer comes in the form of weaponization. Much like the military and camouflage, threat actors don’t want to be noticed.  
  
They want to pair their malicious payload with something that appears normal and benign. **A PDF attachment or a standard Word file can be used to camouflage malicious payloads**, for example.



**3. Delivery: The Path Inside**  
The threat actor has his weaponized payload and now he needs to deliver it.  How is the payload delivered into your system when you are already taking security precautions?

**Threat actors will pair their payloads with actions you take every day**, such as checking your email or visiting a website. Both of these normal processes can be a **gateway for the threat actor.**



**4. Exploitation: Flipping the Switch**Exploitation is what flips the switch, making the threat active. This could be as simple as opening a macro-enabled Word document, **which can execute embedded malicious code**.



**5. Installation: Building a Back Door**   
Malicious code is now running on the system.  The payload can begin installation of an implant, allowing access and the ability to maintain position within your environment.  
  
This essentially acts as a “backdoor” allowing the threat actor to **enter and exit your system whenever he pleases.**



**6. Command and Control: Taking the Wheel**The installed implant now needs to connect to an operator, or in this case, connect to a system that allows **manual or programmatic control of the threat**.   
  
Once the connection is made, access is granted. The threat actor now has the platform in place needed to **begin executing  his objectives.**



**7. Actions on Objectives: Access Granted**  
The attacker can now begin executing his objective.  This may include using the primary access system to **move laterally into other systems within your network.**

