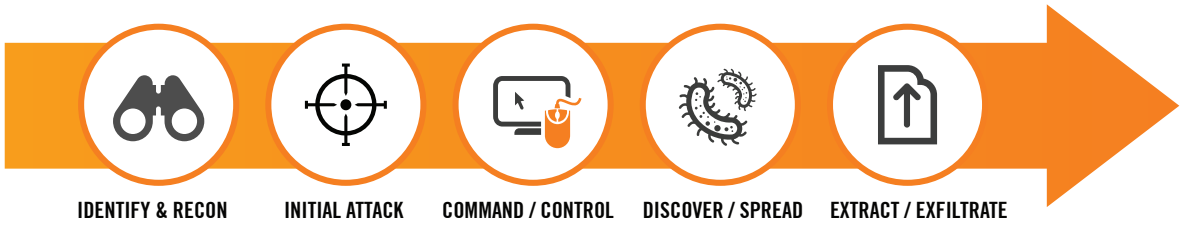
ALERT LOGIC®

DISSECTING RANSOMWARE THROUGH THE CYBER KILL CHAIN®

Fueled by a recent string of technological advancements, ransomware attacks have increased dramatically in terms of both volume and their level of sophistication. A ransomware attack blocks user access to files, data, or entire devices with the intent of extorting a ransom in exchange for restored access. A successful ransomware attack can be devastating to business operations and data integrity.

The Lockheed Martin Computer Cyber Kill Chain® provides a framework for understanding how malware applications target and infect organizations. Specifically applying this methodology to ransomware attacks can enhance your ability to understand how your organization could become a target and help to identify the behavior patterns exhibited by ransomware when attempting to infect host systems.



IDENTIFY & RECON

To identify a target organization or user, ransomware relies mainly on email addresses to deliver the infected payload. Targets can either be chosen at random from mass email lists (spam) acquired through data breaches of other sites or organizations, or they may be specifically targeted through phishing campaigns against a particular organization or individual. Phishing-based ransomware campaigns often rely on data available in open-source professional or personal social media sites. In other examples of ransomware attacks, infected payloads can be delivered through infected websites via web exploit kits, exploiting vulnerabilities in client-side browsers. This type of activity can still be classified as the "recon" stage, given that web exploit kits will still need to identify a browser vulnerability that can be exploited ahead of moving to the next stage, the initial attack.

INITIAL ATTACK

The initial attack is the point at which the infected payload is delivered to the target. As mentioned earlier, the attack tool of choice is often an email with an infected link (to a file or site), or infected attachment (such as a Word document or media file) that requires user interaction (download or open) to ensure successful delivery of the malware application. If we consider another method, such as compromised websites with infected software or applications, the method still relies on file download or installation for successful delivery of the malware application. Less common, however, is delivery of ransomware through infected websites using web exploit kits or the technique known as malvertising. This approach can be very difficult to detect and is often "zero-day" in nature (exploiting browser vulnerabilities that allow download and execution of payloads, often without the user's knowledge).

COMMAND & CONTROL

Once successfully delivered, the ransomware application will almost always attempt to communicate with its command network (also known as C2 activity), an external IP or domain address through which it attempts to relay data relevant to the infected host system(s), and in some cases retrieve encryption key data. The challenge for most ransomware writers is that embedded public key encryption requires a different key for each infection, so the trend is the download of key data from the C2 infrastructure. This ensures further reliance on malicious IPs and the anonymization of network communication to operate effectively within the targeted environment.

DISCOVER & SPREAD

Few ransomware variants today operate on a self-propagation basis once a particular host becomes infected. In fact, the "spread" phase is normally achieved lower down in the chain, through the initial attack vectors used by the malware, such as email, compromised websites, or downloaded applications. However, there are ransomware variants that will attempt to infect system files and spread to other hosts within the infrastructure, and a new era of "CryptoWorms" is expected to surface as malware writers become more sophisticated or existing campaigns become less effective over time.

EXTRACT & EXFILTRATE

The extract phase in ransomware can be viewed from two different angles:

1. The ransom payment itself (Bitcoin)
2. The ability to find or extract key les for encryption as part of its propagation capabilities on the infected system.

In many cases, when the extract phase is reached in the kill chain it is already too late. Without access to the decryption keys, not much can be done to mitigate the infection on the affected hosts. Ransomware will work to target species or directories on a host system, specifically searching for data of interest that will help ensure a successful ransom demand and resulting payment. The latest versions of ransomware are becoming more effective at extracting data for encryption from system and user directories.