More than any other form of malware, ransomware remains to be one of the most dangerous and persistent threats to enterprises today. In the year 2020 alone, many brands such as Jack Daniels and Garmin disclosed that their data was breached and encrypted by diverse groups of cybercriminals all over the world.

Though a lot of attention regarding ransomware has been given to the way in which attackers phish their way into a network, one of the crucial aspects of ransomware attacks if less talked-about i.e. attacker dwell time. As the name suggests, it refers to the duration of time an intruder enters a network and stays undetected.

For most part of the last few years, most of the ransomware attacks would be of typical nature, where an attacker would successfully deploy malicious files to encrypt data on numerous machines as fast as possible before it would reveal itself as a successful attack by locking the screens of victims. However recently, ransomware criminals lurk around in networks and quietly spy around on your data, waiting to get their hands on information of higher value to get more compensation.

Although the average attacker dwell time of ransomware attacks is comparatively lesser than that of other malware, every single day that it dwells undetected in your network presents a higher threat to you in terms of your information and financial assets.

**A New Era of Cyber Attacks**

The last decade has seen ransomware becoming the preferred mode of cyber attacks for criminal organizations and hackers. This is because the security teams have multiple variants to protect their network against, while at the same time cyber criminals have also learnt more innovative and sophisticated ways.

One such example of ransomware is Sodinokibi, where the threat actors succeeded to invent new ways for maximizing their returns by stealing the data and then crypto-locking the victim’s systems, while threatening them to leak or sell their data elsewhere in case they were not paid the ransom amount.

Another example is that of the REvil group, which has made ransomware an easy to learn and use commodity for newbie hackers by selling their malware services on subscription. Not only do they earn by selling, they are also making money by offering further affiliate programs and getting commission from every successful attack made as a result of their subscription.

Furthermore, an increased in remote work and [online shopping](http://www.cardzgroup.com/ContactLessSmartCard.html) due to the recent pandemic, these groups now have more opportunities to exploit known security vulnerabilities in remote desktop protocols and exploiting poor security controls of organizations unfamiliar with security practices.

**Why is Attacker Dwell Time an Important Metric?**

Just as ransomware groups have shifted their focus from quantity to quality, security teams should also adopt a mindset where they assume that the threats actors are already inside their network, rather than thinking to keep them out.

What attackers stay undetected inside networks they weeks or even months to explore in detail, learning how to exploit privileges and use them to their own benefit by pushing ransomware into maximum possible endpoint devices. They can also utilize this time to learn about important network resources like sensitive data storage segments, system backups and other vital systems that they can exploit to make their ransomware attack more successful and bring them more financial gains.

**How to Reduce Attacker Dwell Time?**

While it’s a good practice to prevent malicious actors from entering your network, it’s not always that easy or entirely possible. The best prevention is to assume they are already inside. Considering this scenario, you can reduce the attacker dwell time by adopting some important measures such as:

**Measuring Compromise Intentionally**

For organizations, performing threat hunting and penetration testing regularly is an essential security practice. Adopting and measuring compromise continuously can enable security teams to gather event management and network feeds and measure their level of compromise in terms of smaller segments.

**Correlating Network Intelligence**

Cybercriminals use the network as their entry point and to communicate with command servers as they exfiltrate data eventually. This movement leaves behind metadata scraps, whether from scanning firewalls for open ports or from resolving a DNS query. When you correlate these scraps into an integrated view, it is easier for network defenders to determine when the network is communicating outside of their system.

**Implement a Zero-Trust Framework**

Zero-trust model works more effectively from the perspective of ransomware attacks as compared to conventional trust-but-verify model with software-defined layer enforcing micro-segmentation and access with least privilege across networks. This makes it harder for attackers to jump across a network and escalate privilege.

As criminals continue to invent new ways to breach and infiltrate into a network to plant their ransomware attacks, the real challenge is not only in stopping them from entering but also in exposing blind spots in network to avert minor attacks from causing harm at a bigger scale.