Remote Encryption Attacks Surge: How One Vulnerable Device Can Spell Disaster

Ransomware groups are increasingly switching to remote encryption in their attacks, marking a new escalation in tactics adopted by financially motivated actors to ensure the success of their campaigns.  
"Companies can have thousands of computers connected to their network, and with remote ransomware, all it takes is one underprotected device to compromise the entire network," Mark Loman, vice president of threat research at Sophos, said.   
"Attackers know this, so they hunt for that one' weak spot' — and most companies have at least one. Remote encryption is going to stay a perennial problem for defenders."  
Remote encryption (aka remote ransomware), as the name implies, occurs when a compromised endpoint is used to encrypt data on other devices on the same network.  
 UPCOMING WEBINAR Beat AI-Powered Threats with Zero Trust - Webinar for Security Professionals Traditional security measures won't cut it in today's world. It's time for Zero Trust Security. Secure your data like never before. Join Now   
In October 2023, Microsoft revealed that around 60% of ransomware attacks now involve malicious remote encryption in an effort to minimize their footprint, with more than 80% of all compromises originating from unmanaged devices.  
"Ransomware families known to support remote encryption include Akira, ALPHV/BlackCat, BlackMatter, LockBit, and Royal, and it's a technique that's been around for some time – as far back as 2013, CryptoLocker was targeting network shares," Sophos said.  
A significant advantage to this approach is that it renders process-based remediation measures ineffective and the managed machines cannot detect the malicious activity since it is only present in an unmanaged device.  
The development comes amid broader shifts in the ransomware landscape, with the threat actors adopting atypical programming languages, targeting beyond Windows systems, auctioning stolen data, and launching attacks after business hours and at weekends to thwart detection and incident response efforts.  
  
Sophos, in a report published last week, highlighted the "symbiotic – but often uneasy – relationship" between ransomware gangs and the media, as a way to not only attract attention, but also to control the narrative and dispute what they view as inaccurate coverage.  
This also extends to publishing FAQs and press releases on their data leak sites, even including direct quotes from the operators, and correcting mistakes made by journalists. Another tactic is the use of catchy names and slick graphics, indicating an evolution of the professionalization of cyber crime.  
  
"The RansomHouse group, for example, has a message on its leak site specifically aimed at journalists, in which it offers to share information on a 'PR Telegram channel' before it is officially published," Sophos noted.  
While ransomware groups like Conti and Pysa are known for adopting an organizational hierarchy comprising senior executives, system admins, developers, recruiters, HR, and legal teams, there is evidence to suggest that some have advertised opportunities for English writers and speakers on criminal forums.  
"Media engagement provides ransomware gangs with both tactical and strategic advantages; it allows them to apply pressure to their victims, while also enabling them to shape the narrative, inflate their own notoriety and egos, and further 'mythologize' themselves," the company said.  
  
  
Found this article interesting? Follow us on Twitter  and LinkedIn to read more exclusive content we post.

Link https://thehackernews.com/2023/12/remote-encryption-attacks-surge-how-one.html