Ransomware Is Not APT, and It Requires A Different Strategy

chris.rohlf@gmail.com

The United States is no stranger to dealing with Advanced Persistent Threats (APT) in cyber. Intrusions by APT actors are so pervasive and harmful that they've become a top national security priority over the last decade. But the APT acronym doesn't capture intent, just their supposed technical sophistication and persistent nature in pursuit of a specific intelligence goal. Regardless, APT has come to be synonymous with 'nation state' or 'state-sponsored' actors. The US Government's strategy for response has likewise evolved over that time, with concepts such as Defend Forward and Persistent Engagement defining the conversation.

The technical implementation of the offensive component of the Defend Forward strategy often entails burning adversary operations, tactics and techniques, toolchains, and Command and Control (C2) infrastructure by publishing Indicators of Compromise (IOC) and detailed analysis to the public. This strategy is built upon the assumption that these operations are sensitive, costly, and involve a fair amount of planning and risk. APT actors are not opportunistic in nature; they target specific entities and organizations, and their failure to deliver intelligence, or expose the interests of whichever state is behind it, can potentially incur a high cost. The Defend Forward strategy has a lot of value where these assumptions hold.

Ransomware has also become a top national security priority. In October 2021, the United States convened an international summit amongst partner nations to discuss how we might combat this problem. But ransomware is a different animal from APT, which is primarily driven by intelligence collection goals. Even in cases where a host government turns a blind eye to these activities they are still fundamentally different at the technical and operational level. Ransomware operations often involve separate groups of actors whose only link is financial in nature, ephemeral infrastructure that is easily reproduced, poor opsec, and generally lower end technical capabilities than that of their APT cousins.

Perhaps the most defining trait of ransomware groups is the opportunistic nature of their crimes. They target hospitals, schools, and businesses alike, which is precisely why the threat has morphed into a national security concern. A more sophisticated ransomware group may estimate who is most likely to pay, or use financial data to determine what price to demand. Recent developments have also included an extortion component where victims are threatened with the release of their data to the public unless the ransom is paid. The goal is to extract as much money as possible from victims, no matter who those victims are or what downstream effect it may have. The prevalence of crypto currencies has made these crimes instant, and anonymous enough that determining attribution through the traditional financial system is extremely difficult. Instead, we rely on sophisticated methods that analyze and track relationships between wallets and transfers of crypto on the public blockchain. This is essential because these actors quickly distribute and disperse these funds across many wallets, or launder them through gaming or offshore accounts, making these funds difficult to recover.

Some have called for applying the Defend Forward strategy against ransomware groups as a means for disrupting and deterring their behavior, and making victims whole. This might take the form of recovering the crypto currency ransom sent by the victim by gaining access to cryptographic private keys of the wallets these funds were transferred to. We saw this happen in the Colonial Pipeline ransomware incident earlier this year when US Law Enforcement announced they had recovered $2.3 million USD in ransom payments. One can dream up many ways in which the FBI gained access to this key, but wallets are temporary and easy to recreate, so this strategy may not scale very well.

Many ransomware attacks rely on simple phishing strategies, misconfigurations of complex enterprise software like Active Directory or Remote Desktop, or publicly known vulnerabilities their victims have yet to patch. There is limited opportunity to burn the tooling used to conduct these operations as they often use open source tools, or utilities already present on the system once they gain access. But what other techniques might the U.S. Government apply to ransomware actors from its Defend Forward strategy?

Taking down ransomware infrastructure is one option, but in many cases it’s only needed for launching the initial compromise of victims. Where extortion tactics are employed this strategy may have more value. Ransomware groups have to exfiltrate data before they can extort victims with its release. At the end of the day these operators can easily spin up new infrastructure anywhere in the world.

Ransomware groups are often composed of multiple teams divided up into those who develop and supply the tools, those who execute the initial compromise, and those who extract and manage the funds. Like any sprawling operation opsec failures among these groups is a weak link worth targeting. Pushing for KYC (Know Your Customer) style requirements at crypto exchanges around the world may create some friction on the process of extracting funds from victims, but it’s only effective if you know the identities of these actors. Uncovering the identity of those involved, and where they physically reside, is obviously essential for building a strong criminal case, but often these groups are based in places outside the reach of law enforcement. Putting pressure on these crypto exchanges is a viable tactic we should pursue. But trafficking in stolen identities and accounts has been a staple of the cyber criminal element for a long time.

The Defend Forward strategy is designed for countering and disrupting APT style actors, but its value in combating ransomware operators is not yet clear. There are complications around the legal authorities of those tasked with executing the Defend Forward strategy against what are essentially criminal actors and not nation state adversaries. This detail may become less of an issue as the problem morphs into a national security concern. But what priority should this take over countering APT actors? Whenever the USG chooses to apply offensive operations against a ransomware group they run the risk of exposing a capability of their own that could be utilized elsewhere. Given the low cost for ransomware actors to achieve operational status even after a successful disruption campaign this risk may not be worth it.

The ease at which hospitals, local and state governments, schools, and small businesses are compromised is a failure we must own, and correct. Multi factor authentication, and faster patch timelines sound easy but can be difficult to implement for organizations with little to no IT staff let alone dedicated security teams. These basic cyber hygiene practices won't solve the ransomware problem but they will crimp the long tail of unsophisticated groups. We shouldn't lose sight of that value, we should double down on the investment and lower the cost of defense for everyone. It scales better than any short lived win offensive actions can achieve.

There is no single solution to ransomware, we should reach for every lever possible to combat it. We can remove one set of threat actors today but another can take their place tomorrow unless we get a handle on the vulnerabilities that enable them. We should be careful not to view the problem exclusively through a threat actor lens or over-value what role offensive operations can have against actors that are ultimately unphased even when we succeed at disrupting their operations.