KCS Group Europe

GozNym and the rise of competitive malware

23rd May 2019

An organised criminal gang using the GozNym malware to collectively steal over $100m USD has been dismantled. Working across six countries and two continents, at least ten gang members have now been charged with theft and laundering worldwide. But while the immediate threat of GozNym may be over, it is far from the end of the story for cybercrime, or malware-as-a-service.

GozNym worked on a fundamental level, like much other malware: a combination of two separate strands, one (Nymaim) dropping ransomware onto the device in the first place and the other (Gozi) performing the actual act of theft. The two have both been around for many years, although the melding into GozNym itself is relatively recent.

What is notable is the degree to which this was malware-as-a-service. The ringleaders scoured the dark web looking for those hackers advertising the services and skills they needed: essentially visiting the world's largest job fair and handpicking their favourites. Not only does this instantly raise the threat potential of the fraud, enabling it to reach worldwide and be much more technically proficient, but it is indicative of the growing cyber-crime trend of advertising, and contracting out, hackers for hire. These operations are thus more professional, broad in scope and more dedicated – a genuine 'team effort' that is instantly more serious and dangerous than the traditional image of the 'lone wolf' hacker. Crime is a business just like any other and the use of the dark web to recruit, plan and act enables a stronger class of criminal.

The targets of GozNym were the standard sample one would expect small and medium enterprises, legal firms, and global corporates, enough of a wide cross-section to allow for several bites of the apple but still carefully targeted so as to have financial reserves worth stealing. This is of course to say nothing of the possibility that the financial frauds themselves may have been (very well-paid) diversions from hiding other, information-gathering malware on the infected systems which is likely to be even more beneficial in the long-term.

As cyber-crime becomes even more decentralised, global and professionalised, it is to be expected that such attempts, and the networks behind them, will become the norm. The difficulty is in meeting these in a manner appropriate to both scope and scale. If the threat comes from an OCG that could very well have government backing or support, or at the very least a harvested selection of experienced and skilful hackers deliberately recruited, it is clear that attacks can be launched on a scale and with a seriousness that companies may not be prepared for. Not only is it crucial for 'reactive' cyber-defences to be in place, in terms of firewalls, quarantines, education and the like, but there must be greater efforts made at proactivity, to determine what kinds of groups are gathering on the Dark Web and what their targets are, to determine the means and motives of these professional cyber-criminals. The sale of services and recruitment will not abate; all that remains is for corporates to ensure that their mitigation is equally professional.