WHAT WOULD A DIGITAL SANCTIONS REGIME RELYING ON MALWARE LOOK LIKE?

A day ago, the second ransomware based on NSA tools leaked by Shadow Brokers hit. The attack was focused on Ukraine, in large part because "patient zero" appears to be a tax software update for a Ukrainian company M.E.Doc. But global giants include Maersk and Merck were also affected. Russian oil giant Rosneft was affected too, though there are conflicting claims about how badly it was disabled.

A day in, folks still can't get a grasp on this attack, even down to the name (it started as Petya until security folks determined it's not the ransomware of the same name, leading to the use of NotPetya).

While using far more attack vectors (and more toys from Shadow Brokers), this attack bears two similarities with last month's WannaCry attack: the ransom requested $300 to decrypt locked data, and the ransom function was never really designed to work properly.

> There is mounting evidence that the #GoldenEye / #Petya ransomware campaign might not have targeted financial gains but rather data destruction.
>
> - *The choice of a regular, non-bulletproof e-mail service provider to act as a communication channel was obviously a wrong decision in terms of business.*
> - *The lack of automation*

> *in the payment & key retrieval process makes it really difficult for the attacking party to honor their end of the promise.*
> - *There is a total lack of usability in the payment confirmation: the user has to manually type an extremely long, mixed case "personal installation key" + "wallet" is prone to typos.*
>
> Update 6/28 06.00 GMT+3
>
> The email address that was used by the threat actors to get payment confirmations has been suspended by Posteo. This means that all payments made overnight will be unable to get validated, and therefore will surely not receive the decryption key. Not that we have ever advised otherwise, but if you're planning to pay the ransom, stop now. You'll lose your data anyway, but you'll contribute in funding the development of new malware. Even so, there have been 15 payments made after the suspension of the e-mail address. The wallet now totals 3.64053686 BTC out of 40 payments, with a net worth of $US 9,000.

Indeed, Matt Suiche argues the attack is better thought of as a wiper attack, designed to destroy rather than lock data, than a ransomware attack.

It will take some time to understand what the

attack really is, particularly given the degree to which it appears to masquerade as things it's not. But for the moment, I want to consider how a similar attack might be used as a counter to sanctions regimes. As far as we currently know, this attack made doing business with Ukraine a very expensive business proposition, as doing business with, say, some oligarchs in Russia is made costly for those subject to US sanctions because have to bank in the US. The attack served as a self-executing investigative method to identify just who had business tax dealing in Ukraine, and imposed an immediate cost. So whether or not that's what this *is*, such an attack could be used to counteract sanctions imposed by the international banking community.

Again, I'm just spitballing.

But some dates are of interest.

On June 14, the Senate passed some harsh new sanctions on Russia, ostensibly just for Russia's Ukrainian and Syrian related actions, not for its tampering in last year's US election. The House mucked up that bill, but the Senate will continue to try to impose new sanctions. Trump might well veto the sanctions, but that will cause him a great deal of political trouble amid the Russian investigation.

The Petya/NotPetya malware was compiled on June 18.

Microsoft dates the attack to June 27 at 10:30 GMT.

> We observed telemetry showing the MEDoc software updater process (*EzVit.exe)* executing a malicious command-line matching this exact attack pattern on Tuesday, June 27 around 10:30 a.m. GMT.

Today, June 28, is a public holiday in Ukraine, making it more difficult to deal with the attack.

Again, I’m not saying that’s what NotPetya is. I am saying that if you wanted to design a counter to financial sanctions using malware, NotPetya is close to what it’d look like.