Who's behind the GPcode ransomware?

zdnet.com/article/whos-behind-the-gpcode-ransomware/

In one of these moments when those who are supposed to know, don't know, and those who don't realize what they know

aren't reaching the appropriate parties, it's time we get back to the basics - finding out who's behind GPcode, and trying to tip them on the consequences of their blackmailing actions in between collecting as much actionable intelligence as possible using OSINT (open source intelligence) and CYBERINT (cyber intelligence practices).

Great situational awareness on behalf of Kaspersky Labs who were the first to report that a new version of GPcode (also known as PGPCoder) is in the wild, this time with a successful implementation of RSA 1024-bit encryption. However, aiming to crack the encryption could set an important precedent, namely using distributed computing to fight the effect of cyber criminal's actions. Theoretically, the next time they'll introduce even stronger encryption, which would be impossible to crack unless we want to end up running a dedicated BOINC project cracking ransomware in the future. Are there any other more pragmatic solutions to dealing with cryptoviral extortion? It's all a matter of perspective. More info on the Stop GPcode initiative, seeking and receiving the collective intelligence of independent researchers in this blog post :

> "Along with antivirus companies around the world, we're faced with the task of cracking the RSA 1024-bit key. This is a huge cryptographic challenge. We estimate it would take around 15 million modern computers, running for about a year, to crack such a key. Of course, we don't have that type of computing power at our disposal. This is a case where we need to work together and apply all our collective knowledge and resources to the problem. So we're calling on you: cryptographers, governmental and scientific institutions, antivirus companies, independent researchers…join with us to stop Gpcode. This is a unique project – uniting brain-power and resources out of ethical, rather than theoretical or malicious considerations. Here are the public keys used by the authors of Gpcode."

Despite that GPcode indeed got the encryption implementation right this time, it's only weakness remains the way it simply deletes the files it has just encrypted, next to securely wiping them out - at least according to a single sample obtained. Consequently, just like a situation where your files are encrypted with strong encryption and virtually impossibe to crack, but the original files Moreover, instead of trying to crack an algorithm that's created not to be cracked at least efficiently enough to produce valuable results by have the encrypted data decrypted, why not buy a single copy of the decryptor and start analyzing it? It also appears that the decryptor isn't universal, namely they seem to be building custom decryptors once the public key used to encrypt the data has been provided to them.

So, the ultimate question - who's behind the GPcode ransomware? It's Russian teens with pimples, using E-gold and Liberty Reserve accounts, running three different GPcode campaigns, two of which request either $100 or $200 for the decryptor, and communicating from Chinese IPs. Here are all the details regarding the emails they use, the email responses they sent back, the currency accounts, as well their most recent IPs used in the communication :

Emails used by the GPcode authors where the infected victims are supposed to contact them : content715@yahoo .com saveinfo89@yahoo .com cipher4000@yahoo .com decrypt482@yahoo .com

Virtual currency accounts used by the malware authors : Liberty Reserve - account U6890784 E-Gold - account - 5431725 E-Gold - account - 5437838

Sample response email : "*Next, you should send $100 to Liberty Reserve account U6890784 or E-Gold account 5431725 (www.e-gold.com) To buy E-currency you may use exchange service, see or any other. In the transfer description specify your e-mail. After receive your payment, we send decryptor to your e-mail. For check our guarantee you may send us one any encrypted file (with cipher key, specified in any !_READ_ME_!.txt file, being in the directorys with the encrypted files). We decrypt it and send to you originally decrypted file. Best Regards, Daniel Robertson*"

Second sample response email this time requesting $200 : "*The price of decryptor is 200 USD. For payment you may use one of following variants: 1. Payment to E-Gold account 5437838 (www.e-gold.com). 2. Payment to Liberty Reserve account U6890784 (www.libertyreserve.com). 3. If you do not make one of this variants, contact us for decision it. For check our guarantee you may send us ONE any encrypted file. We decrypt it and send to you originally decrypted file. For any questions contact us via e-mail. Best regards. Paul Dyke*"

So, you've got two people responding back with copy and paste emails, each of them seeking a different amount of money? Weird. The John Dow-ish Daniel Robertson is emailing from **58.38.8.211** (Liaoning Province Network China Network Communications Group Corporation No.156,Fu-Xing-Men-Nei Street, Beijing 100031), and Paul Dyke from **221.201.2.227**(Liaoning Province Network China Network Communications Group Corporation No.156,Fu-Xing-Men-Nei Street, Beijing 100031), both Chinese IPs, despite that these campaigners are Russians.

This incident is a great example of targeted cryptoviral extortion attacks, namely, it's not efficiency centered and the core distribution method remains unknown for the time being. Analysis and investigation is continuing. If you're affected, look for backups of your data, or try restoring the deleted files, don't stimulate blackmailing practices by paying them.