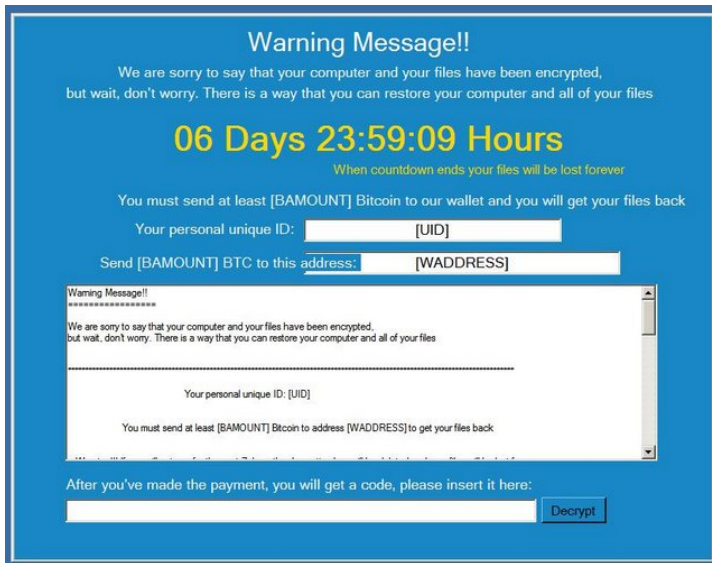


Pour récupérer vos données, ce ransomware vous demande d'infecter d'autres victimes

<h3>Restoring your files - The fast and easy way</h3> <p>To get your files fast, please transfer 1.0 Bitcoin to our wallet address 1LEiPgvh8S9VEXWV2aZTytSRd7e9B1bVWt3. When we will get the money, we will immediately give you your private decryption key. Payment should be confirmed in about 2 hours after payment made.</p> <h3>What we did?</h3> <p>We had encrypted all of your important images, documents, videos and all other files on your computer. We used a very strong encryption algorithm that used by all governments all over the world (Encryption -Wikipedia). We store your personal decryption code to your files on our servers and we are the only ones that can decrypt your files. Please don't try to be smart, anything other than payment will cause damage to your files and the files will be lost forever!!!</p> <p>If you will not pay for the next 7 days, the decryption key will be deleted and your files will be lost forever.</p>	<h3>Restoring your files - The nasty way</h3> <p>Send the link below to other people, if two or more people will install this file and pay, we will decrypt your files for free.</p> <p>https://3hnuhydu4pd247qb.onion.tor/r/De72bfe849c71dec4a867fe60c78ffa5</p> <h3>Why we do that?</h3> <p>We are a group of computer science students from Syria, as you probably know Syria is having bad time for the last 5 years. Since 2011 we have more the half million people died and over 5 million refugees. Each part of our team has lost a dear member from his family. I personally have lost both my parents and my little sister in 2015. The sad part of this war is that all the parts keep fighting but eventually we the poor and simple people suffer and watching our family and friends die each day. The world remained silent and no one helping us so we decided to take an action. (Syria War in Wikipedia)</p> <p>Be perfectly sure that all the money that we get goes to food, medicine, shelter to our people. We are extremely sorry that we forcing you to pay but that's the only way that we can keep living.</p>	<p>Pour récupérer vos données, ce ransomware vous demande d'infecter d'autres victimes</p>
--	--	--

Un nouveau logiciel de rançon contraint ses victimes à participer à sa propagation, sous peine de perdre leurs données.



L'idée semble tout droit sortie d'un épisode de *Black Mirror*. Il y a quelques jours, l'équipe de MalwareHunterTeam a mis la main sur un *malware* en cours de développement, baptisé Popcorn Time – aucun lien avec l'application de streaming du même nom. Comme de nombreux logiciels de rançon, il demande à ses victimes de payer pour pouvoir déchiffrer leurs données. Le tarif est fixé à un Bitcoin, soit 730 euros au cours actuel. Mais l'équipe de Popcorn Time laisse une possibilité moins coûteuse, qu'elle qualifie elle-même de «sale»: propager le logiciel en infectant deux autres personnes. Les données sont déverrouillées après le paiement des nouvelles victimes.

Restoring your files - The fast and easy way To get your files fast, please transfer 1.0 Bitcoin to our wallet address 1LEiPavh559vEXWV2az7y1SRd7e9B1bVW3 . When we get the money, we will immediately give you your private decryption key. Payment should be confirmed in about 2 hours after payment made.	Restoring your files - The nasty way Send the link below to other people, if two or more people will install this file and pay, we will decrypt your files for free. https://3thnuhydu4pd247qb.onion/tor10e72bf6f49c71dec4a867fe60c78ffa5
What we did? We had encrypted all of your important images, documents, videos and all other files on your computer. We used a very strong encryption algorithm that used by all governments all over the world (Encryption -Wikipedia). We store your personal decryption code to your files on our servers and we are the only ones that can decrypt your files. Please don't try to be smart, anything other than payment will cause damage to your files and the files will be lost forever!!! <small>If you will not pay for the next 7 days, the decryption key will be deleted and your files will be lost forever.</small>	Why we do that? We are a group of computer science students from Syria, as you probably know Syria is having bad time for the last 5 years. Since 2011 we have more the half million people died and over 5 million refugees. Each part of our team has lost a dear member from his family. I personally have lost both my parents and my little sister in 2015. The sad part of this war is that all the parts keep fighting but eventually we the poor and simple people suffer and watching our family and friends die each day. The world remained silent and no one helping us so we decided to take an action. (Syria War in Wikipedia) <small>Be perfectly sure that all the money that we get goes to food, medicine, shelter to our people. We are extremely sorry that we forcing you to pay but that's the only way that we can keep living.</small>

Pour vous aider à choisir la méthode sale, les auteurs de Popcorn Time fournissent le lien sur lequel devront cliquer les cibles. Il redirige vers un fichier hébergé sur un serveur Tor – actuellement hors-service. Une fois exécuté, Popcorn Time prétend installer un logiciel, tout en exécutant le chiffrement. Comme le relève le site Bleeping Computer, il s'attaque à de nombreux dossiers, parmi lesquels Mes Documents, Mes Photos, Ma Musique ou le Bureau. Chaque fichier est chiffré en AES (*Advanced Encryption Standard*). Il affiche ensuite une page d'avertissement incluant l'ensemble des instructions, un décompte d'une semaine et un champ permettant d'inscrire la clé de déchiffrement.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur
: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>

Original de l'article mis en page : Pour récupérer vos données, ce ransomware vous demande d'infecter d'autres victimes