websense®

EXECUTIVE SUMMARY

WEBSENSE SOLUTION FOR RANSOMWARE

websense
TRITON®

'Ransomware' is a type of malware that attempts to extort money from a computer user by infecting and taking control of the victim's machine or the files or documents stored on it. Currently, there are three types of Ransomware: Encryption Ransomware, Lockscreen Ransomware and Master Boot Record Ransomware.

Most Ransomware gets distributed either via email and Web access or by instant messaging or social media. Regardless of it its entry point, it can be difficult to determine if the variant is targeted for specific organisations or individuals. Two specific Ransomware threats that have been in the news lately are Torrentlocker and Cryptolocker. The creators of these Ransomware programs have been emailing them to huge numbers of people and organisations with great success.

Unfortunately, these Ransomware perpetrators have been associated with a variety of other malware as well, such as backdoor Trojans, downloaders, spammers, password-stealers, ad-clickers and the like. These cybercriminals have been both nimble and persistent in creating new variants of their malware, keeping up with changes in protection technology and continually targeting different groups. These clever malware tactics have rendered traditional data security technologies ineffective in defending against them.

Additionally, Lure campaigns have successfully snared many unsuspecting Ransomware victims with legitimate looking and sounding websites and URLs. Once the unsuspecting victim goes to the lure website or URL, the Ransomware trap is sprung. We have seen the following Lure campaigns, in chronological order:

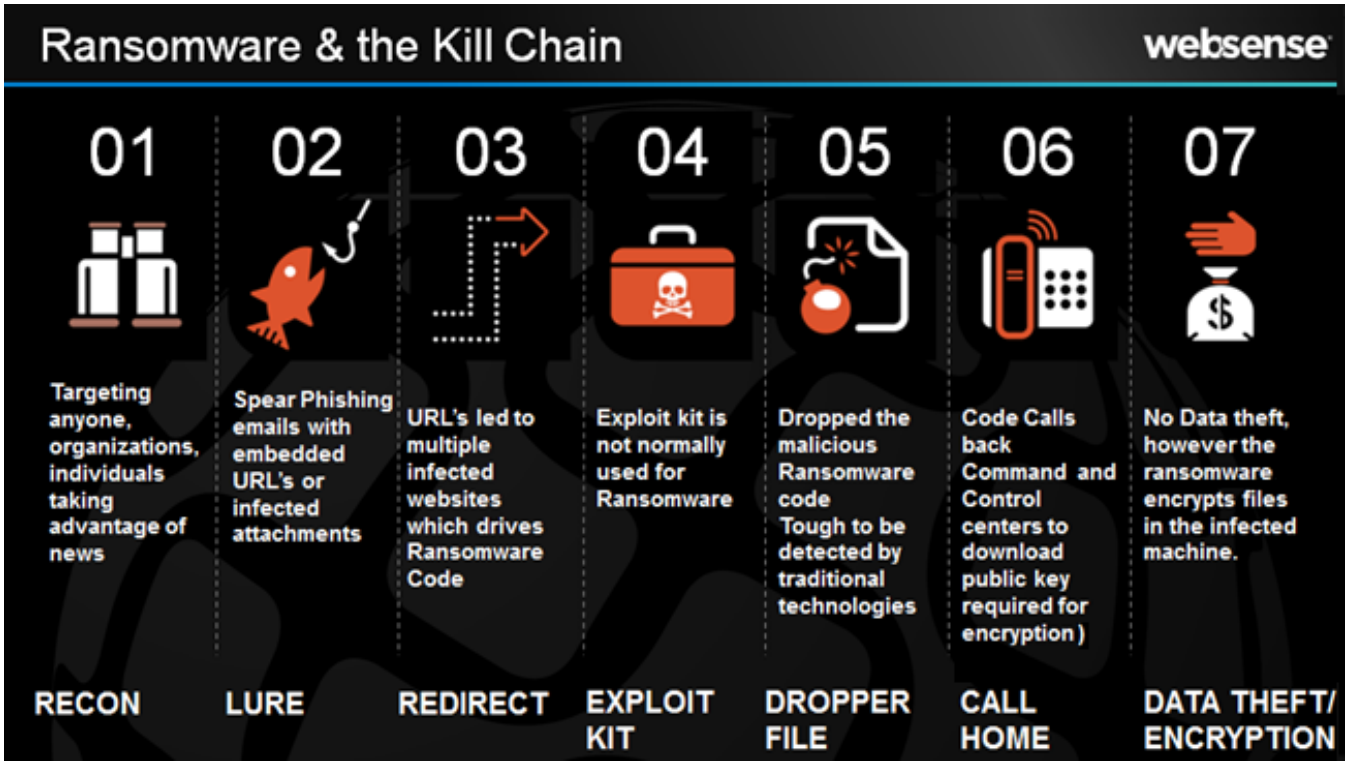
- RoyalMail (directed towards British end-users)
- Auspost
- PostNL (directed towards Dutch end-users)
- Telstra
- E-Parcel Group
- SDRO – NSW Government

These are what we are aware of so far. However, there likely are, or will be, others. The graph below indicates the geographical regions which are most targeted by most Ransomware malware:

EXECUTIVE SUMMARY
WEBSENSE SOLUTION FOR RANSOMWARE

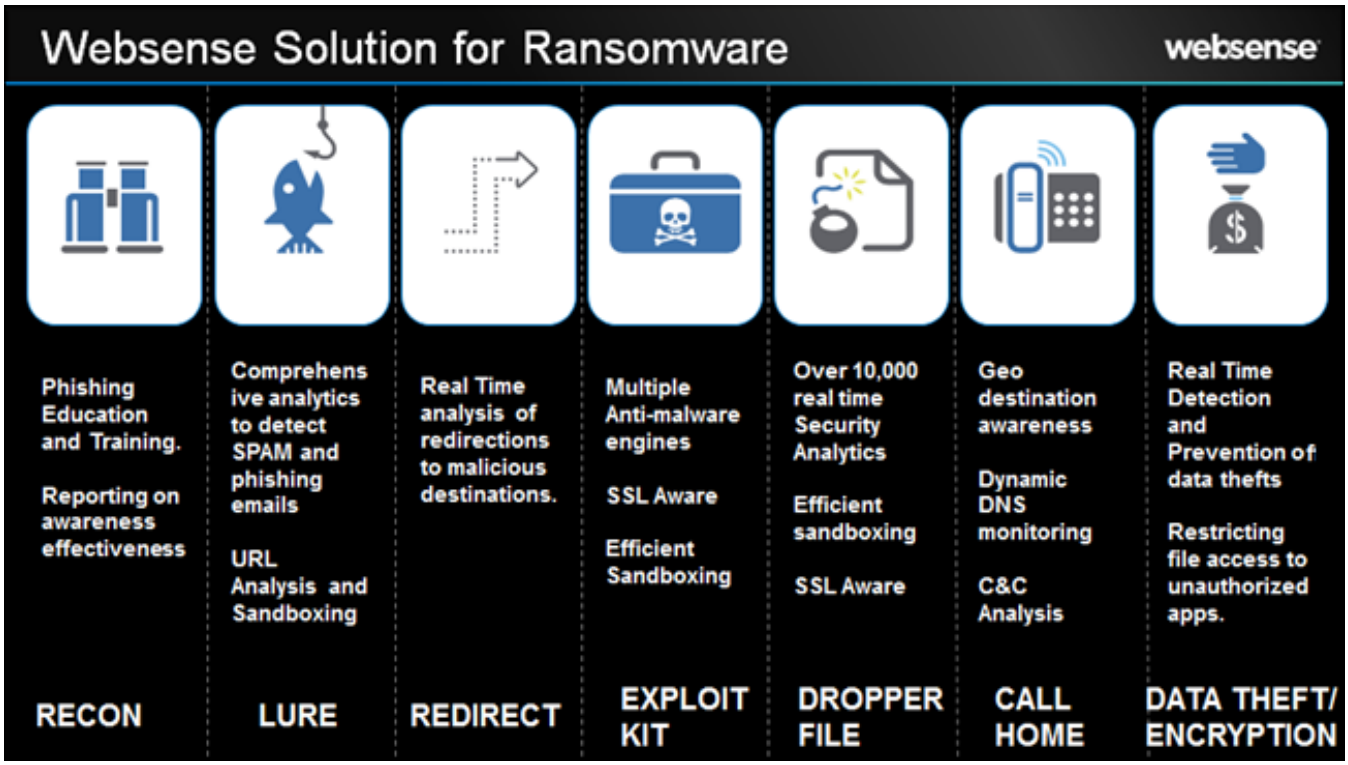
Ransomware authors typically use two types of encryption: the files themselves are protected with 256-bit AES encryption; the keys generated by this first encryption process are then protected with 2048-bit RSA encryption. The malware authors then keep the private key that would allow both the keys on the user's machine and the files they protect, to be decrypted. The decryption key can neither be deciphered by brute-force decryption nor gathered from the affected computer's memory. The Ransomware authors are the only ones who have the private key.

The diagram below indicates how Ransomware fits into the 7-Stage Kill Chain:



More details on the threat lifecycle is available in the white paper in the link:
http://www.websense.com/assets/white-papers/whitepaper-summary-7-stages-data-theft-en.pdf

As a global leader in data security, Websense is uniquely positioned to detect and defend against the various threat stages of Ransomware (Cryptolocker) and protect your data from becoming a cybercriminal hostage. The key capabilities of Websense security solutions to protect your data across the entire 7-Stage Kill Chain are identified below:



Websense Sandboxing efficiently detects Advanced Threats like Cryptolocker and we have successfully blocked this Ransomware threat for several customers. A snapshot of our sandboxing analysis for Cryptolocker is displayed below:

For more details on how Websense can detect and prevent Ransomware infections, please reach out to **websenseconnect@websense.com** or to request your **FREE Cyber Threat Risk Assessment** please visit: **http://www.websense.com/content/cryptolocker-risk-assessment-au.html**


TRITON STOPS MORE THREATS.
WE CAN PROVE IT.
www.websense.com/proveit
websense
TRITON®
[execsum-anz-risk-assessment-241114]