

## **"WannaStart" looking at India and Spain?—?and behind those VPN's?**

*Cyber expert Simon Smith has doubts that the origin really is North Korea. He presents data gathered from a counter social engineering exercise that may uncover hidden treasures.*

**MELBOURNE, Australia - May 24, 2017 - [PRLog](#)** -- When Simon Smith of eVestigator first saw an image of a conversation purporting to be with the ransomware Cybercriminals, his creative mind sparked.

Having no expectations, Mr. Smith wondered what would happen if we could capture as much data as we could from that piece of information. As a social engineering experiment, and in response to intelligence from the email image which appeared to be sent at 9:29 PM referencing an email from thundercrypt@tuta.io to qwe uio in the public domain?—?Mr. Smith decided to create a domain name with privacy called qweuio.com.

This domain name was not advertised and was essentially 'unknown' and was sent to that email address in a tactful manner. Of course, it was a little seed that would sprout and one day tell us about its journey, and what it found along the way.

That it did. It passed through some very interesting channels along the way. The identity of the domain was in some way advertised on Google, despite a negative robots.txt entry ?—?however still nobody knew of this oddly spelt website so the odds were quite good that a click on the site would be from the source. There was always a possibility of an error rate, but that is noticed over time.

Interestingly the first stop was a TOR exit node called EDWARDSNOWDEN2 followed by other TOR exit nodes, then some VPN's.

The TOR locations may be useful for researchers later on. However, Mr. Smith, a Cybersecurity and Cybercrime social engineer from was more interested in the VPN/Proxies that took an interest in this site and encourages the community to expose the addresses behind them. Even more alarming, Mr. Smith identified what was, the first true IP addresses showing Spain and India, multiple times.

Referring back to historical events, raises questions over the recent media in those two countries in relation to hacking, international arrests, or motives for researchers to look at.

The raw metadata can be downloaded free from the eVestigator website. A graphical earth representation is in the final stages which show the events in a very clear timed format.

Mr. Smith urges all VPN providers to cooperate with authorities and expects a degree of error as ironically he did run into other malware companies as he was inspecting the traffic, inspecting him!

Nevertheless, if you do not look or try new methods, you just might never know what information you miss.

Mr. Smith has solved hundreds of Cybercrimes in Australia and across the world and has been known to crack cases with little to no evidence. He gives this data openly to researchers to combine with the other sequences of events to join further intelligence.

He does however want to spread his concern that the links to potentially the US (or the Countries under those very early VPNs), India or Spain cannot go unnoticed.

--- End ---

Source	Simon Smith
Email	<a href="#">Click to contact author</a>
Phone	+61410643121
City/Town	Melbourne
State/Province	Victoria
Country	Australia
Industry	<a href="#">Internet</a>
Tags	<a href="#">Wannacry</a> , <a href="#">Breakingnews</a> , <a href="#">Ransomware</a>
Link	<a href="https://prlog.org/12642087">https://prlog.org/12642087</a>



Scan this QR Code with your SmartPhone to-

- \* Read this news online
- \* Contact author
- \* Bookmark or share online