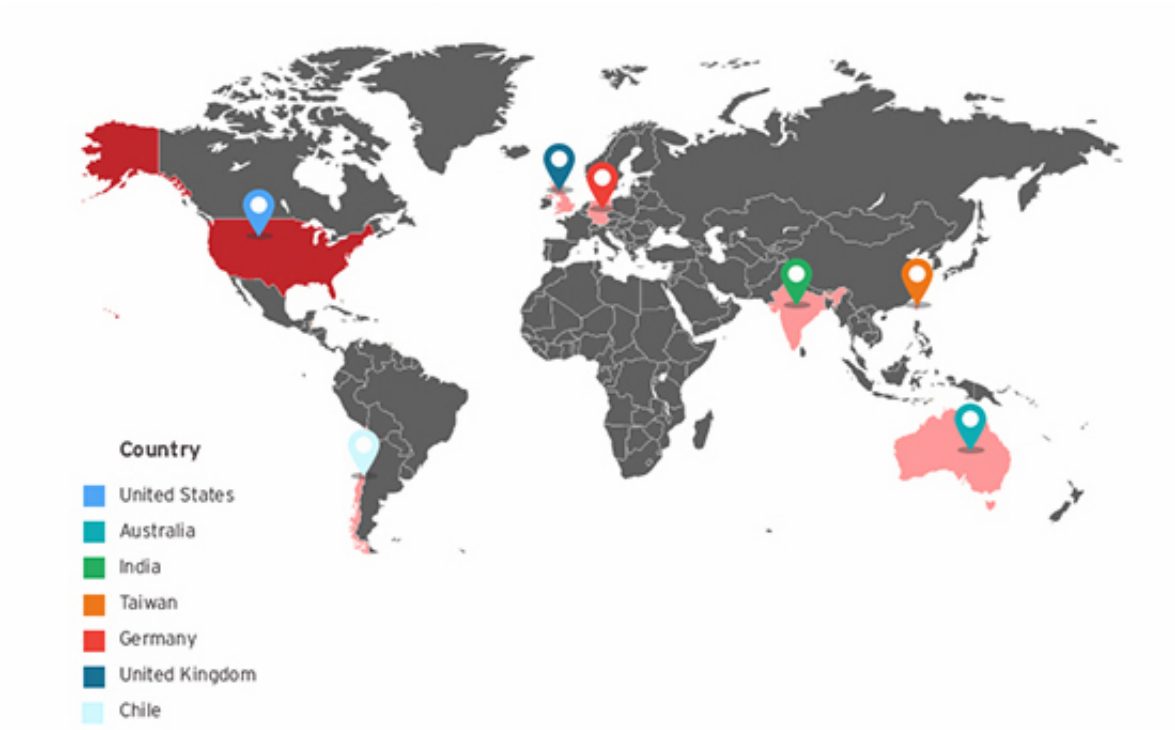
MUST READ Ponmocup, never underestimate a botnet that infected 15 million PCs



Operation Black Atlas, PoS malware is flooding network worldwide

December 3, 2015 By Pierluigi Paganini

Trend Micro uncovered a large-scale operation dubbed Black Atlas operation, in reference to notorious BlackPOS PoS malware.

It's Christmas time also for crooks, in this period the number of credit card breaches and scams increases with alarming punctuality. In the US, we use to assist an increase of credit card breaches involving PoS malware, last victims in order of time are Hilton Hotel and Starwood hotel chains.

In the last weeks, security experts detected a number of new threats in the wild such as Cherry Picker, ModPoS, and Pro Pos.

Not only US retailers are at risk, new threat seeks out PoS systems within targeted networks, small and medium sized business networks all over the world belonging to any various industries.

Experts at Trend Micro uncovered a large-scale operation dubbed operation Black Atlas, in reference to notorious BlackPOS PoS malware that is the threat primarily used in these attacks.

My readers will surely remember that BlackPOS, also known as Kaptoxa, was the malware used during the Target breach in 2013 and attacks on retail accounts in 2014.

Threat actors behind the operation have developed a set of hacking tools used in their operations.

"Operation Black Atlas has been around since September 2015, just in time to plant its seeds before the holiday season. Its targets include businesses in the healthcare, retail, and more industries which rely on card payment systems." reads a blog post published by Trend Micro. "The operation is run by technically sophisticated cybercriminals *who are knowledgeable in a variety of penetration testing tools and possess a wide network of connections to PoS malware in the underground market."*

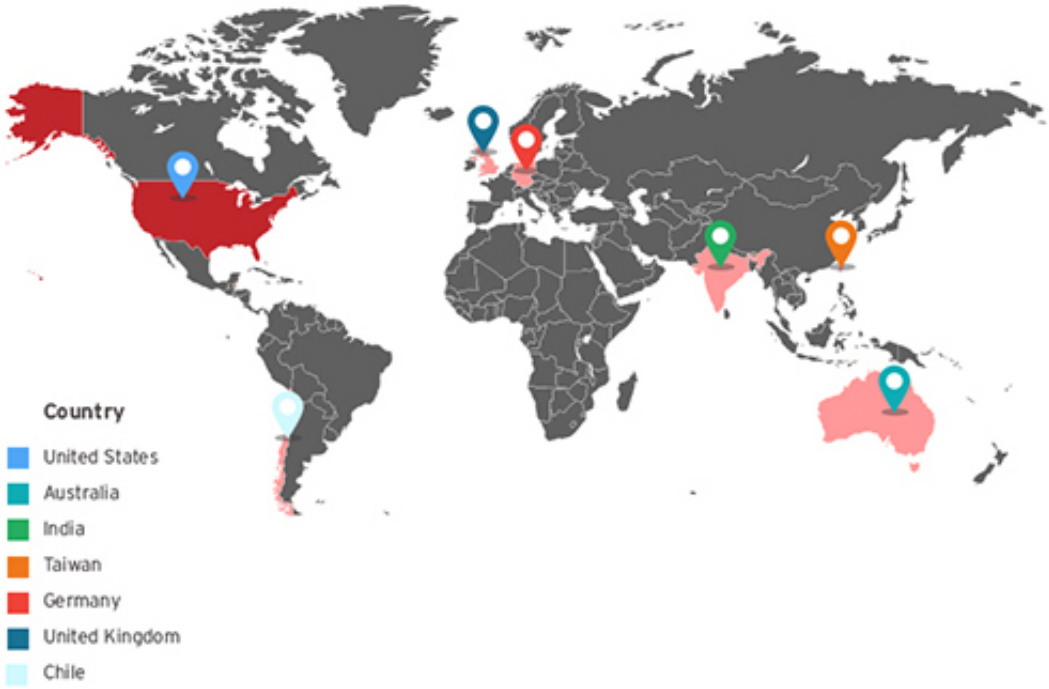
Malware utilized in Black Atlas included a number of popular PoS malware, including Alina, NewPOSThings, a Kronos backdoor, and of course the BlackPOS threat.

Bad actors behind the Black Atlas operation have been able to steal user login credentials of the victims, email accounts, and other sensitive information. The experts also discovered a live video feed of closed-circuit television (CCTV) cameras in a gasoline station, evidence that crooks are collecting whatever information is available.

"Similar to GamaPoS, the Black Atlas operators employed a "shotgun" approach to infiltrate networks as opposed to zeroing in on specific targets. They basically checked available ports on the Internet to see if they can get in, ending up with multiple targets around the world." continues the post.

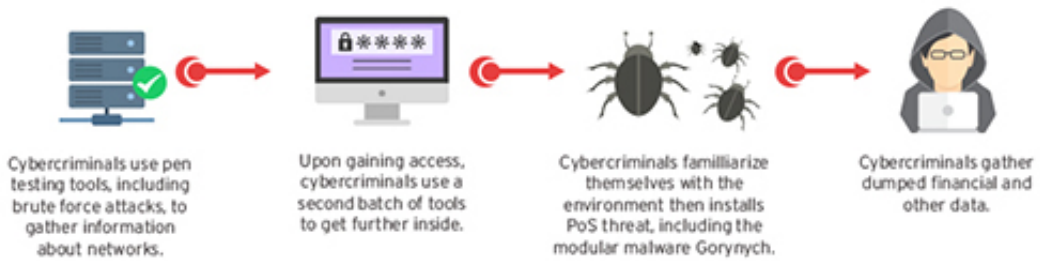
The experts at Trend Micro observed that Black Atlas operators used the botnet Gorynych or Diamond Fox in a number of installations.

In the following image has reported the distribution of Gorynych targets in Operation Black Atlas.



The Operation Black Atlas involved numerous healthcare organization in the US, the experts explained that threat actors use to run an initial intelligence gathering or reconnaissance activity to identify the best system to compromise, that they used the tools to run the attack (i.e. Brute force or dictionary attack).

"Networks with weak password practices are likely to fall victim to this initial penetration testing stage. Many of these tools are easily downloaded from various sites on the Internet. The



In the attack stage the crooks utilized remote access tools to steal more information and move laterally within the network, one inside they inject the PoS threats.

Trend Micro announced it will provide further details about the Black Atlas Operation.

Pierluigi Paganini

(Security Affairs – Black Atlas Operation, Pos Malware botnet)

Share it please ...

Alina | backdoor | Black Atlas Operation | BlackPOS | botnet | Cybercrime | Hacking | Kronos | NewPosThings | POS malware

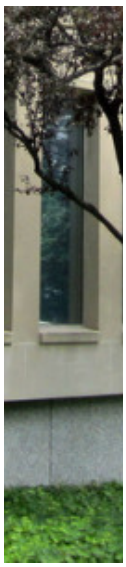
Breaking News | Cyber Crime | Malware

SHARE ON

Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in for , he is r-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and “Digital Virtual Currency and Bitcoin”.

MORE S



China ar
OPM ha
The Chin
arrested
breachin
Manager

PREVIOUS ARTICLE
China arrested hackers suspected of OPM hack

NEXT ARTICLE
3G/4G modems continue to be vulnerable

YOU MIGHT ALSO LIKE

Ponmocup, never underestimate a botnet that infected 15 million PCs

December 4, 2015 By Pierluigi Paganini

3G/4G modems continue to be vulnerable

December 3, 2015 By Pierluigi Paganini