Operation Black Atlas Endangers In-Store Card Payments and SMBs Worldwide; Switches between BlackPOS and Other Tools

- Posted on:December 1, 2015 at 12:31 am
- Posted in:Botnets, Malware
- Author:
  Jay Yaneza (Threats Analyst)

With the coming holidays also come news of various credit card breaches that endanger the data of many industries and their customers. High-profile breaches, such as that of the Hilton Hotel and other similar establishments, were accomplished using point-of-sale (PoS) malware, leading many to fear digital threats on brick-and-mortar retailers this Thanksgiving, Black Friday, Cyber Monday, and the rest of the holiday season. Researchers also found a broad campaign that uses the modular ModPOS malware to steal payment card data from retailers in the US.

However, from what we have seen, it is not only retailers in the US that are at risk of breaches. Our researchers recently found an early version of a potentially powerful, adaptable, and invisible botnet that seeks out PoS systems within networks. It has

already extended its reach to small and medium sized business networks all over the world, including a healthcare organization in the US. We are calling this operation Black Atlas, in reference to BlackPOS, the malware primarily used in this operation.

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.

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. Its operators built a set of tools much like a Swiss army knife, with each tool offering a different functionality. Malware utilized in Black Atlas included (but were not limited to) variants of Alina, NewPOSThings, a Kronos backdoor, and BlackPOS. BlackPOS, also known as Kaptoxa, was the malware used during the Target breach in 2013 and attacks on retail accounts in 2014.

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. The following graph shows where these targets are located:

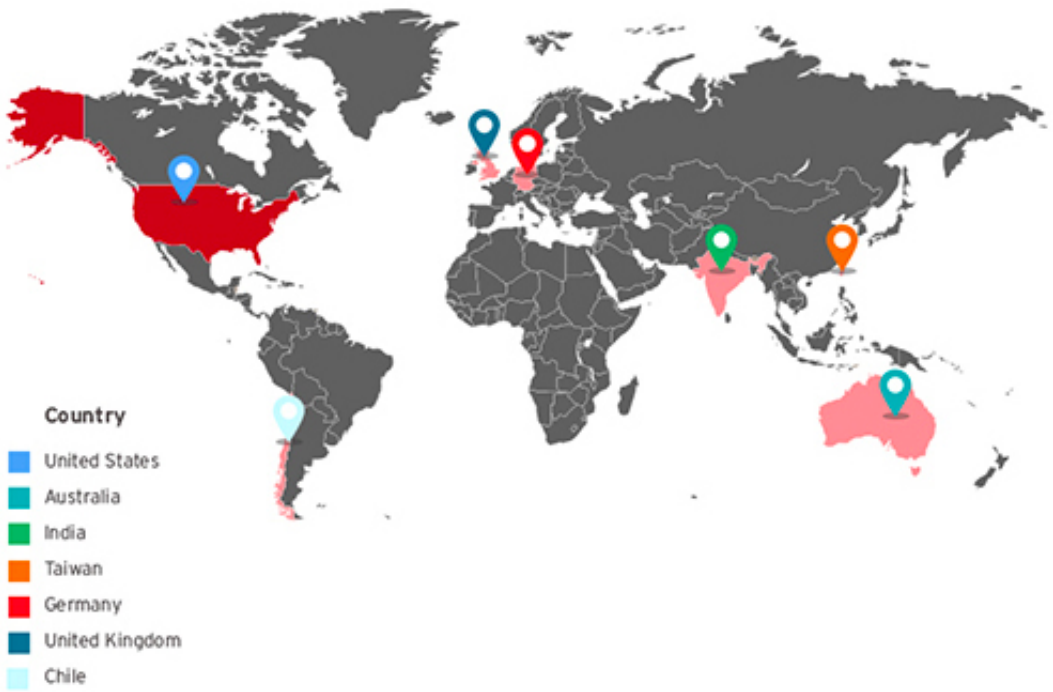


Figure 1. Distribution of Gorynych targets in Operation Black Atlas

So far, the Black Atlas operators have been able to steal user credentials to websites that contain sensitive information, email accounts, and Facebook. The most interesting data we found was that of a live video feed of closed-circuit television (CCTV) cameras in a gasoline station. Either this is taking reconnaissance to another real-time level or the cybercriminals simply captured whatever information is available.

How Operation Black Atlas Works

Our analysis of the attacks against these targets gave us further insights on how the Black Atlas operators seek out PoS systems from networks. In one particular case, which involved a healthcare organization in the US, we found out how the Black Atlas

operators operate.

Similar to a targeted attack, Black Atlas involves an intelligence gathering or reconnaissance period where cybercriminals use a set of tools similar to a Swiss army knife to check how best to infiltrate systems. It also involves the use of tools such as brute force or dictionary attack tools, SMTP scanners, and remote desktop viewers. 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.

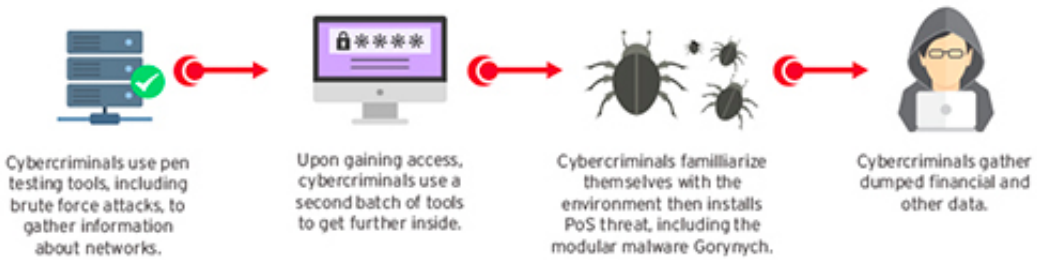


Figure 2. Operation Black Atlas infection chain

The cybercriminals will then create a test plan based on the initial probe, and then use a second set of tools to execute the said plan. In the case of the healthcare organization, the Black Atlas operators utilized remote access tools to steal more information and move laterally within the network. The use of remote access tools at this stage depends on how the target environment is configured, with the method of gaining remote access also varying based on the target.

Once inside, cybercriminals then familiarize themselves with the environment. What follows is the introduction of PoS threats, which the cybercriminals source from the operation's broad Swiss army knife toolbox.The favored way to introduce other tools and threats is via the built-in command-line FTP since antimalware solutions had already blocked the initial site we had reported last September that hosted Katrina and CenterPoS.

Black Atlas operators used the modular botnet Gorynych or Diamond Fox in some installations. Gorynich was used to download a repurposed BlackPOS malware with RAM scraping functionality and upload all the dumped credit card numbers in memory. As the original BlackPOS used a text file to store pilfered credit card data, Gorynych now grabs that text file and does an HTTP POST to complete the data exfiltration:

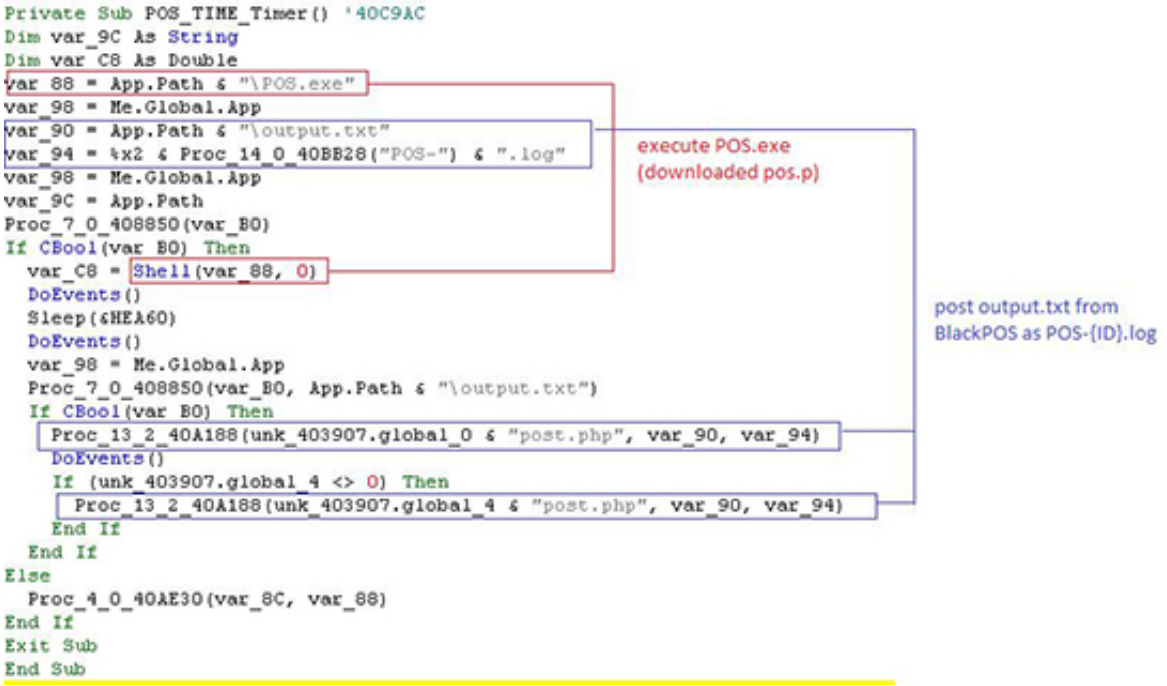


Figure 3. Gorynych data exfiltration stage

In our next blog entry, we will discuss the steps of our investigation, how cybercriminals retrofitted the new Gorynych backdoor to use BlackPOS, and how the whole operation puts a variety of old and new PoS malware at the cybercriminals' fingertips to easily gather financial information. We will also provide technical details, best practices, and recommendations to help IT managers and business owners evade or resolve this PoS threat.

With additional analysis by Erika Mendoza

Related Posts:

- One-Man PoS Malware Operation Captures 22,000 Credit Card Details in Brazil
- Two New PoS Malware Affecting US SMBs
- Credit Card-Scraping Kasidet Builder Leads to Spike in Detections
- Operation Tropic Trooper: Old Vulnerabilities Still Pack a Punch

Tags: Botnetshealthcarepoint-of-salePOSSMB

Featured Stories

- 2016 Predictions: The Fine Line Between Business and Personal
- Pawn Storm Targets MH17 Investigation Team
- FBI, Security Vendors Partner for DRIDEX Takedown
- Japanese Cybercriminals New Addition To Underground Arena
- Follow the Data: Dissecting Data Breaches and Debunking the Myths

Recent Posts

- Operation Black Atlas Endangers In-Store Card Payments and SMBs Worldwide; Switches between BlackPOS and Other Tools
- CTO Insights: Encryption Works – Don't Break It!
- DRIDEX Spam Runs Resurface Against US Targets
- Prototype Nation: Emerging Innovations in Cybercriminal China
- Trend Micro, NCA Partnership Leads to Arrests and Shutdown of Refud.me and Cryptex Reborn

2016 Security Predictions

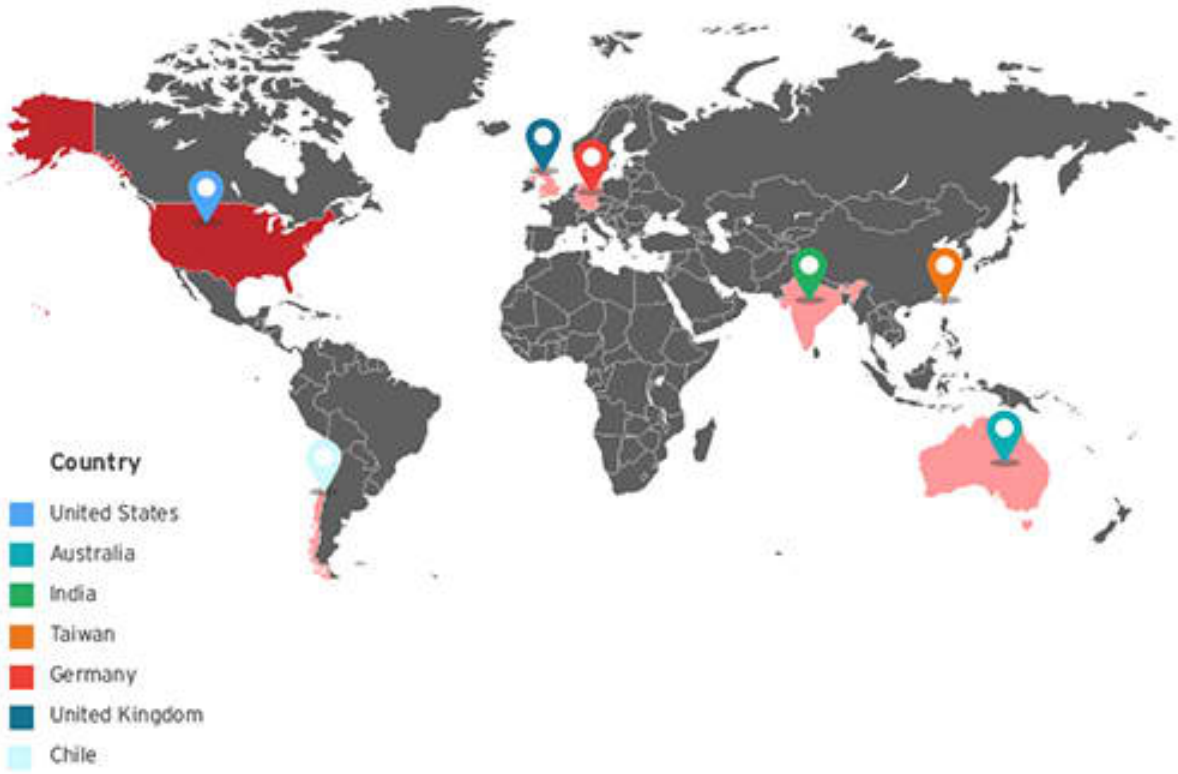
- From new extortion schemes and IoT threats to improved cybercrime legislation, Trend Micro predicts how the security landscape is going to look like in 2016. Read more

Popular Posts

Setting the Record Straight on Moplus SDK and the Wormhole Vulnerability
Cybercriminals Improve Android Malware Stealth Routines with OBAD
Trend Micro, NCA Partnership Leads to Arrests and Shutdown of Refud.me and Cryptex Reborn
Hacking Team Flash Zero-Day Integrated Into Exploit Kits
Siri's Flaw: Apple's Personal Assistant Leaks Personal Data

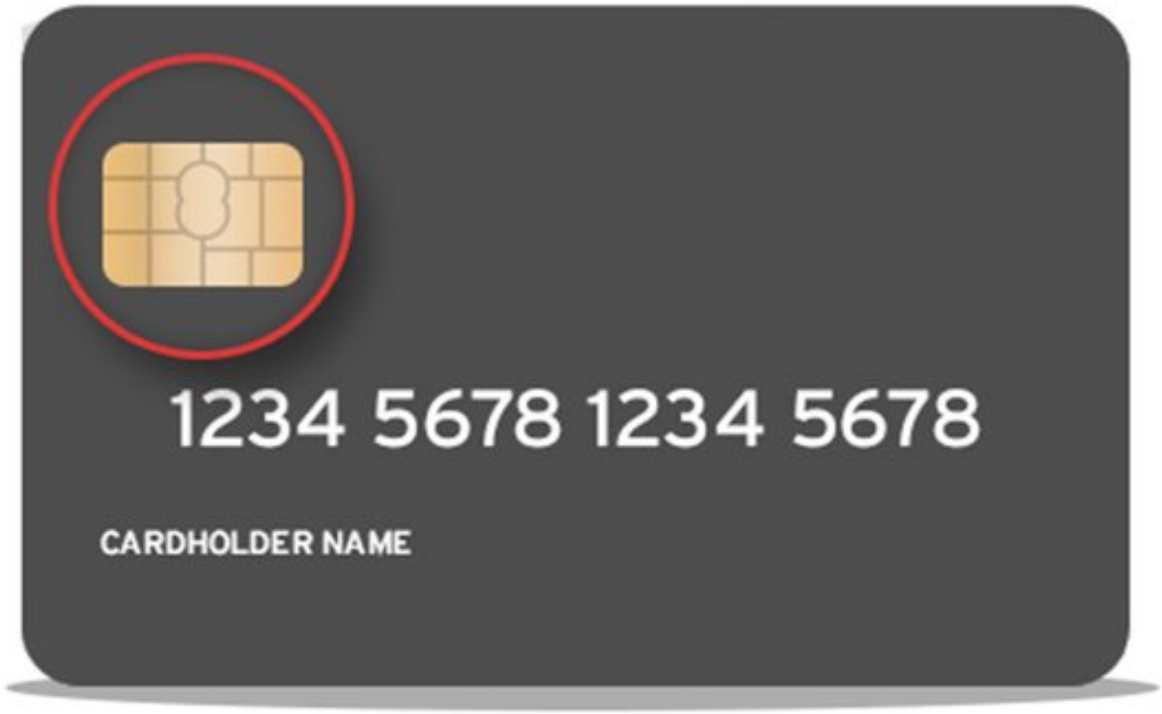
Latest Tweets

- Operation Black Atlas Endangers In-Store Card Payments and SMBs Worldwide: blog.trendmicro.com/trendlabs-secu…



about 7 hours ago

- What does an EMV card look like? Learn more about this payment technology here: trendmicro.com/vinfo/us/secur…



about 15 hours ago
- Encryption works, and is a fundamental part of data protection today. Don’t break it. More from our CTO here: blog.trendmicro.com/trendlabs-secu…
about 1 day ago

Stay Updated

Email Subscription

Your email here

Subscribe

- Home and Home Office
- |
- For Business
- |
- Security Intelligence
- |
- About Trend Micro

- Asia Pacific Region (APAC): Australia / New Zealand, 中国, 日本, 대한민국, 台灣
- Latin America Region (LAR): Brasil, México
- North America Region (NABU): United States, Canada
- Europe, Middle East, & Africa Region (EMEA): France, Deutschland / Österreich / Schweiz, Italia, Р о с с и я, España, United Kingdom / Ireland

- Privacy Statement
- Legal Policies