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

Posted on: December 18, 2015 at 6:21 am

Posted in: Botnets, Malware

Author: Erika Mendoza and Jay Yaneza (Threats Analysts)

This is the second part of our two-part blog series on Operation Black Atlas. The first blog entry is entitled, ***Operation Black Atlas Endangers In-Store Card Payments and SMBs Worldwide; Switches between BlackPOS and Other Tools****.*

Operation Black Atlas has already spread to a multi-state healthcare provider, dental clinics, a machine manufacturer, a technology company focusing on insurance services, a gas station that has a multi-state presence, and a beauty supply shop. It continues to spread across small and medium-sized businesses across the globe, using the modular Gorynych/Diamond Fox botnet to exfiltrate stolen data.

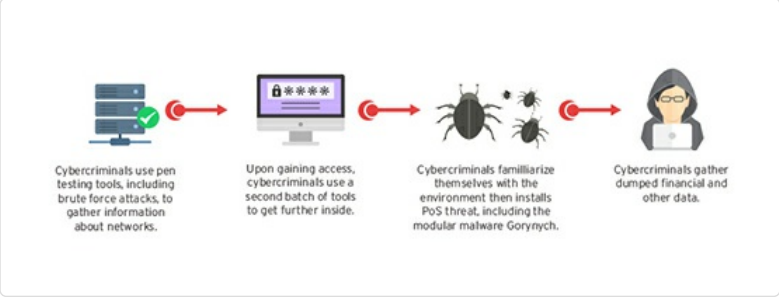


Figure 1. Operation Black Atlas infection chain

Initial Compromise via Pen Testing Tools

The operation uses a variety of penetration testing tools that are available online to probe and penetrate their target's environment. The first set of tools is for scanning and creating a test plan, and often uses brute-force or dictionary attacks to break passwords. The second set of tools is for executing the plan, and mainly targets remote access services, like the VNC Viewer, the remote desktop protocol (RDP), and the built-in Windows Remote Desktop Connection (RDC).

All that stands between the organization and the attacker is a weak password. It is harder to determine lateral movement once user credentials are stolen and used, because the tools used would not be considered malicious. Network defenders must enforce stricter policies on password creation and maintenance or deploy password manager software. They can also configure breach detection systems to log activities like port or vulnerability scanning or brute-force attempts for inspection.

BITS and Pieces of POS and Spying Threats

Once the cybercriminals have scoped the network, they will then introduce PoS threats. They do this by abusing a legitimate function, the Windows Background Intelligent Transfer Service (BITS) or *bitsadmin.exe,* which can be used to transfer files to and from Microsoft and is typically used to download updates to systems. It can easily bypass firewalls and has long been used by malware to sneak in malicious downloads.

In the case of Black Atlas, cybercriminals use BITS to download NewPOSThings, a PoS malware family notable for its RAM scraper, keylogger, keep-alive reporting, and data transfer routines. The operation can also load a variant of Neutrino or Kasidet which has PoS card-scraping functionality. We also saw BlackPOS, CenterPOS, Project Hook, and PwnPOS being used in cases related to the operation. All these PoS threats are available in the cybercriminals' servers.

As such, IT administrators should stay up to date on known and latest PoS malware. We have provided a complete list of indicators of compromise (IOCs) that can betray the presence of these threats in the *Recommendations* section below.

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

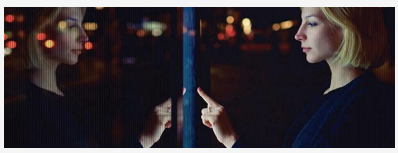
New Targeted Attack Group Buys BIFROSE Code, Works in Teams

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 42 mins ago

Gorynych Rigged for BlackPOS Functions

There's a new player in the card theft game that changes it altogether: Gorynych or the Diamond Fox botnet malware. BKDR_GORYNYCH may not technically be considered a PoS malware, as it is not entirely designed for PoS systems and is also being used outside of the Black Atlas operation. However, cybercriminals running Black Atlas have built a copy that can specifically look for the output file of the BlackPoS malware, which is the one that harvested the credit card data from the targets in the first place. The fact that the images in Gorynych's control panel were named "Kartoxa," which also refers to BlackPoS, further proves the link between the two malware and the operation.

Aside from the PoS plugin, other modules usually downloaded from a subdirectory in the C&C server make up this malware's entirety. These include plugins for getting screenshots, passwords, mails, and more. Without the plugins, Gorynych routines mostly focus on anti-analysis, information theft, and installations. In the Diamond Fox builder, the keylogger and PoS grabber functionalities are disabled by default. However, with Operation Black Atlas, these options were turned on, which proves that cybercriminals running this are intentionally targeting PoS systems.

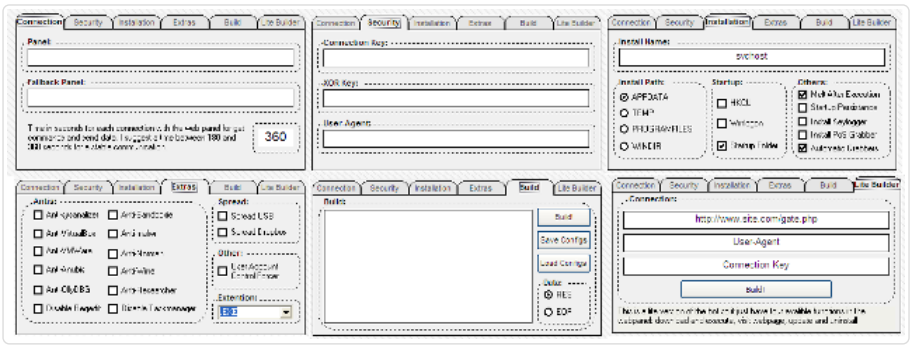


Figure 2. Diamond Fox or Gorynych builder

After downloading its plugins, Gorynych reports to its server via gate.php using HTTP POST. It uses its own user-agent that can be found in its configuration file. The parameters consist of system information used to profile the bot, mainly for identification in the Gorynych control panel. The posted information is encrypted using a simple XOR operation. Hashes, addresses, and other indicators related to Gorynych can be found in the IOC document provided below.

Recommendations

Every network has its own nuances and patterns. As such, applying a single PoS strategy and hoping for the best is out of the question. Our prior research on PoS threats showed us that the best way to handle them is by evaluating which best known strategies and defensive technologies can best enhance the existing network environment.

Trend Micro is monitoring this ongoing activity, and will make follow-up reports on this if necessary. Additional technical details can be found in the Technical Brief. The indicators of compromise are uploaded in the Black Atlas IOC document.

Network segmentation and isolation of cardholder data environment from other networks should be standard for organizations of all sizes. For large organizations, it is important to eliminate unnecessary data and monitor what's left. It is also best to ensure that essential controls are running via regular security checks. IT admins need to monitor and mine event logs.

Meanwhile, smaller organizations should implement a firewall or ACL on remote access services and change default credentials of PoS systems and other internet-facing devices. They should also ensure that third party vendors handling the items mentioned have efficiently done them. However, other essential controls on passwords and network/system security and monitoring of logs used by larger organizations can also be applied. No matter what the size of the organization, what's important is to evaluate your threat landscape to prioritize your treatment strategy.

To enhance the network's security posture on point-of-sale systems, IT admins can read about 26 defensive technologies and strategies outlined in our paper, **Defending Against PoS RAM Scrapers: Current Strategies and Next-Gen Technologies** as well as our write-up on **Protecting Point of Sales Systems from PoS Malware**.

To stop breaches on point-of-sale systems (or any other PoS environment, for that matter), Trend Micro™ Custom Defense™ employs a family of solutions that can detect, analyze, and respond to advanced malware and other attack techniques. Endpoint Application Control can reduce attack exposure ensuring that only updates associated with whitelisted applications can be installed, helping you safeguard your data and machines against unauthorized access and user error.

Related Posts:

- Operation Black Atlas Endangers In-Store Card Payments and SMBs Worldwide; Switches between BlackPOS and Other Tools
- One-Man PoS Malware Operation Captures 22,000 Credit Card Details in Brazil
- Looking Back (and Forward) at PoS Malware
- Operation Woolen-Goldfish: When Kittens Go Phishing

Tags: Targeted Attack | botnet | POS | BlackPOS | Operation Black Atlas | gorynych