THE CIA HIVE COMPONENT

NETWORK SECURITY – UNIVERSITÀ DELLA CALABRIA

PROJECT BY GIADA GABRIELE AND MICHELE MORELLO

THE CIA HIVE COMPONENT

April 14th, 2017, WikiLeaks publishes six documents from the CIA's HIVE project created by its "Embedded Development Branch" (EDB). HIVE is a multi-platform CIA malware suite and its associated control software. The project provides customizable implants for Windows, Solaris, MikroTik (used in internet routers), Linux platforms and a Listening Post (LP)/Command and Control (CA) infrastructure to communicate with these implants.

THE CIA HIVE COMPONENT

Hive can serve multiple operations using multiple implants on target computers. Each operation anonymously registers at least one cover domain for its own use. The server running the domain website is rented from commercial hosting providers as a VPS and its software is customized according to CIA specifications. These servers are the public-facing side of the CIA back-end infrastructure and act as a relay for HTTPS traffic over a VPN connection to a "hidden" CIA server called 'Blot'.

THE CIA HIVE COMPONENT

The cover domain delivers 'innocent' content if somebody browses it by chance. A visitor will not suspect that it is anything else but a normal website. The only peculiarity is not visible to non-technical users: a HTTPS server option that is not widely used - Optional Client Authentication. Hive uses it so that the user browsing the website is not required to authenticate but implants talking to Hive do authenticate themselves and can therefore be detected by the Blot server.

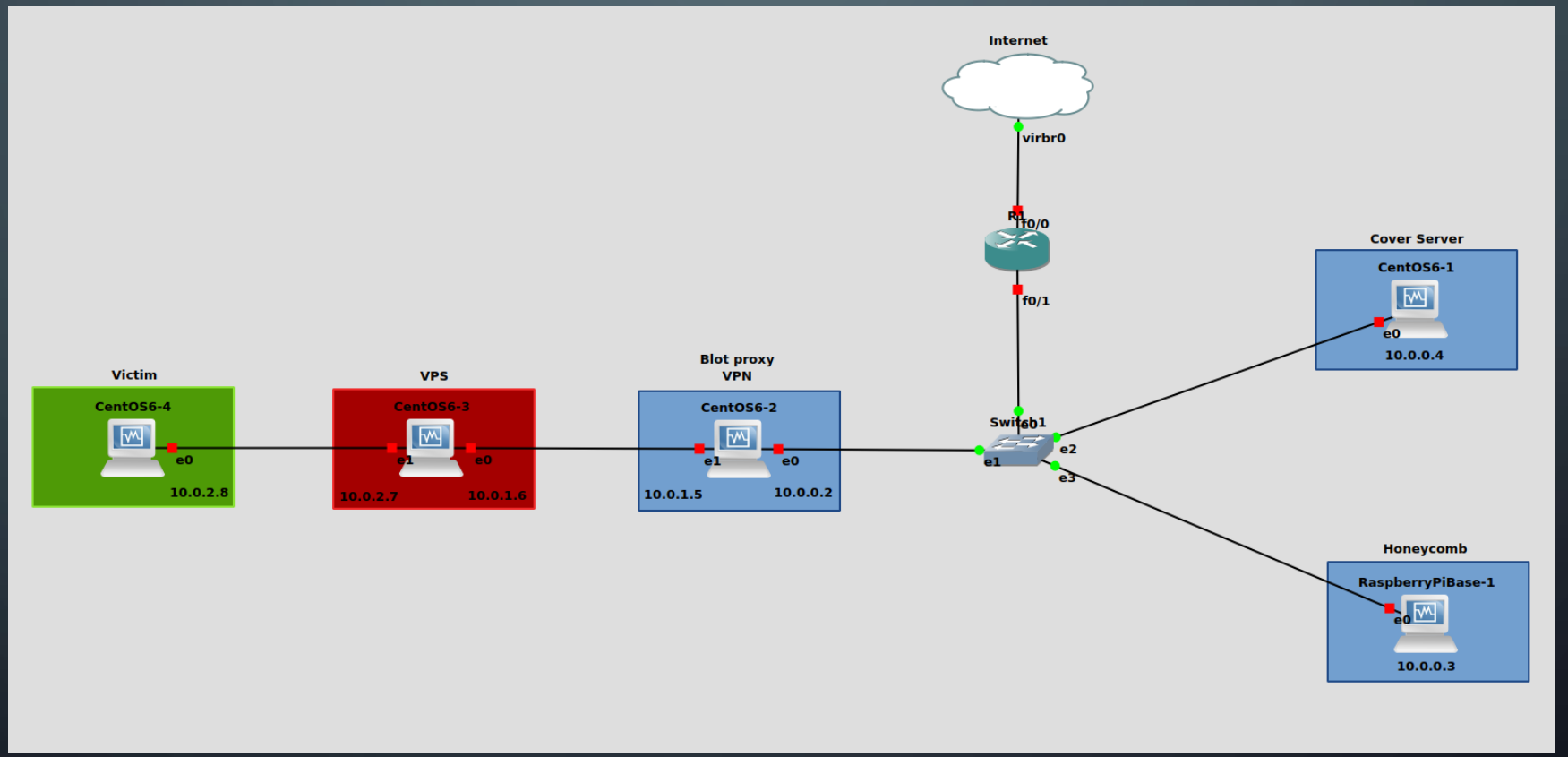
THE CIA HIVE COMPONENT

Traffic from implants is sent to an implant operator management gateway called Honeycomb while all other traffic go to a cover server that delivers the insuspicious content for all other users. The Honeycomb toolserver receives exfiltrated information from the implant; an operator can also task the implant to execute jobs on the target computer, so the toolserver acts as a command-and-control server for the implant.

THE CIA HIVE COMPONENT

The Hive implant communicates with the operator over an SSL-secured tunnel. After the implant is triggered, it calls back to the Swindle/Blot (LP) and receives a server certificate and a certificate authority (CA) certificate which it validates. Once the SSL tunnel is established, the client and the implant perform a Diffie-Hellman key exchange to establish a shared secret key. This key is used to create a second layer of encryption using the AES algorithm.

THE CIA HIVE COMPONENT



THE CIA HIVE COMPONENT – TECHNICAL ASPECTS

BEACONS INFRASTRUCTURE

Patched or unpatched implants are provided by the generator application. Implants will detach from the user's terminal and fork into the background. The goal is for the operator to have a consistent user experience, regardless of the implant's operating system. On the wire, the implant mimics a SSLv3 handshake with Swindle and then sends a small amount of encrypted data to the tool handler.

BEACONS INFRASTRUCTURE

The encrypted beacons consist of the Swindle Tool ID, system uptime, and MAC address. The beacon parameters cannot be changed dynamically by the hive tool handler. To change the beacon parameters, the implants need to be re-patched with new parameters and re-deployed, or in the case of unpatched implants, they need to be restarted with new command line arguments.

BLOT PROXY

Hive beacons were designed to work with the Blot proxy. Beastbox is the proxy router used in the Blot system. Beastbox receives packets from the outside network and presents them to an Implant Traffic Detector (ITD) that is associated with the corresponding transport protocol. Blot looks for a tool ID embedded in the HELLO packet of an SSL session initiation. If the ID is found, then it forwards the packet to the tool-handler, otherwise it is sent to the cover server.

BLOT PROXY

The data contained within this packet is constant except for a time stamp taken from the real-time clock and a few bytes of random data. A CRC checksum is computed from the entire packet and is included with the HELLO packet. When Blot receives this packet, it checks the CRC searches a list of previously seen packets for any matches. If a match is found the packet is assumed to be a TCP replay and is dropped.

BLOT PROXY

Beacon routers are connected to the Switchblade proxy through VPN tunnels to provide security and privacy. Each beacon router/domain has its own dedicated interface and address on the Switchblade. A beacon arriving at a beacon router is routed to the Switchblade which authenticates the implant client's certificate.

BLOT PROXY

Authenticated beacon packets are then routed on to the Honeycomb tool-handler; all others are routed to a cover server corresponding to the domain of the beacon router. The configuration of Switchblade and its peer components allows the egress source address of beacon to be maintained through to the tool-handler or cover server for logging purposes.

HONEYCOMB

Honeycomb is a server application that handles the beacons proxied from Swindle. The Honeycomb server can be configured to start the tool handler automatically at system start. Upon receiving a beacon, Honeycomb will parse-out the MAC address, public IP address, and uptime of the implanted box.

HONEYCOMB

Honeycomb will then write out a ".rsi" file that is one-way transferred for ingestion into Ripper Snapper (a database). The implant ID used in the Ripper Snapper files is the unformatted MAC address of the implanted box. As of Hive 2.0 additional survey data are collected from the beacon.

HONEYCOMB

Hive v2.0 functionality was added to Honeycomb so that it will keep a basic log of beacons that are received. Every beacon will have a log entry created that contains a timestamp of when the beacon was received, the MAC address, public IP address, and the version of the implant that beaconed. In addition, for Hive v2.0 beacons and later, there will be a flag related to which OS the beacon came from.

VICTIM, VPS AND COVER SERVER

*The **victim** of course doesn't know anything, it's a passive protagonist. **VPS** is a server that redirect the victim to the Blot proxy through a VPN tunnel. The **cover server** is a dummy server that receives all the victim's unsuspicious traffic.*

TRIGGERS

The Hive client establishes an interactive session with the implant by sending it a trigger. Starting with Hive version 2.7 only two trigger types are supported: raw-tcp and raw-udp. The raw-udp trigger can be sent to any UDP port on the target system. The raw-tcp trigger can be sent to any open and listening port on the target system. The Hive implant watches for trigger packets in the incoming flow of network traffic.

TRIGGERS

This "sniffer" behavior can be slightly different on each operating system. On Linux and MikroTik, Hive listens on all physical interfaces. Once the implant receives a valid trigger, it pulls the callback IP address and port from the trigger packet, waits a default delay, and then calls back to the listening Hive client. Once connected, the implant and Hive client perform a TLS handshake and initializes an AES encrypted session.

THE CIA HIVE COMPONENT – DEMO