Experts use internet routers to protect web from Angler malware's lures

October 14 2015, by Andrew Smith

Credit: Rebeccarawrr, CC BY

It may not be a household name like Microsoft, Apple or Sony, but Cisco Systems is almost the same size. Cisco is the world's largest supplier of networking equipment such as routers and switches which plug together the various networks that make up the internet. This puts them in the position of being able to use the enormous distribution of their equipment to disable a major ongoing malware attack, Angler.

The Angler exploit kit is software used by hackers to breach and take control of computer systems, known as a tool kit. There have been many such kits over the years, for example in the 1990s the notorious Back Orifice (a pun on Microsoft Backoffice) offered hackers easy to use tools to remotely control Windows computers. Angler is one of the most advanced and widespread today.

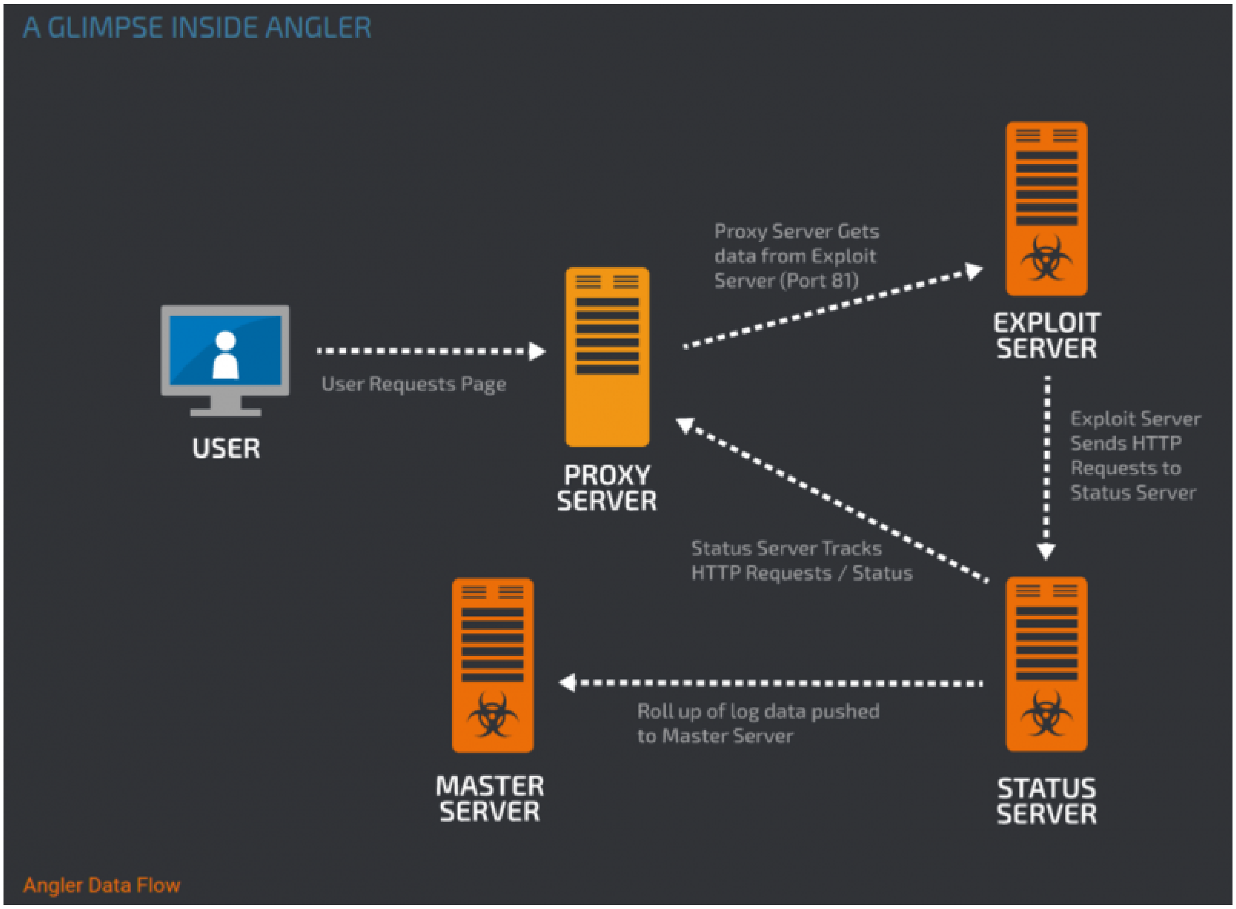
Creating a tool kit and distributing it freely on the internet provides expert tools to wannabe hackers – known as "script kiddies" – who don't necessarily have the skills themselves nor the opportunity to access systems to practice and hone their own hacking techniques. Angler is such a kit, used to create back doors by taking advantage in flaws in popular browser plug-ins such as Flash and Java. Remote access and control of a PC gives hackers the opportunity to take the computers hostage and demand ransom money from their victims, or to steal personal data to be used for fraud or sale.

The security experts investigating Angler estimated that it targeted around 90,000 computers a day, with an estimated fraudulent income of US$30m. As tool kits can be updated, their creators can usually provide work-arounds for each defence created by security software companies, which makes preventing the attacks difficult. While security firms are excellent at spotting variants and updating their database definitions to ensure antivirus software recognises them, not everyone updates in time (or at all) and there is always a new attack being developed.

Cisco's intervention

Cisco helped solve this problem, together with major internet service provider Level 3 Communications, by collecting and analysing Angler's network traffic to discover where it was headed and to tackle the problem at its source. The researchers discovered that the code that compromised targeted computers was located on an exploit server, to which the tool kit installed on compromised computers communicated via a network of proxy servers designed to hide and protect it.

By tracing where Angler's traffic was headed, Cisco and the researchers were able to release updates for its network equipment in use worldwide that would block Angler's attempts to communicate with its servers. The team also contacted the hosting companies with what they'd learned, which then shut down the rogue servers. Cisco has done an outstanding job, as this will make it difficult to use Angler in its current form. However it's unlikely this will be the last we hear it – Angler's creators and maintainers will have to work hard to adapt it to work around the blocks installed on millions of routers worldwide, but will inevitably do just that. The game of cat and mouse will continue.


A GLIMPSE INSIDE ANGLER
USER
User Requests Page
PROXY SERVER
Proxy Server Gets data from Exploit Server (Port 81)
EXPLOIT SERVER
Exploit Server Sends HTTP Requests to Status Server
Status Server Tracks HTTP Requests / Status
STATUS SERVER
Roll up of log data pushed to Master Server
MASTER SERVER
Angler Data Flow

Angler tool kit connects to exploit server via many proxies to hide its route. Credit: TalosIntel

Of course, however much security companies or police and investigators work to try to combat malware and hacking attacks, it's up to you to make sure your antivirus software is installed and up-to-date. If your computer is ever held to ransom, don't provide any financial information – it's better to wipe your computer and start again than to hand your financial details to unknown criminals to be exploited. And of course having back-ups of essential data, such as on cloud services, means it's easier to recover in a worst-case scenario.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation

Citation: Experts use internet routers to protect web from Angler malware's lures (2015, October 14) retrieved 12 May 2024 from https://phys.org/news/2015-10-experts-internet-routers-web-angler.html