The Italian Connection: An analysis of exploit supply chains and digital quartermasters

AUGUST 10, 2015

by Ned Moran and Ben Koehl

On July 5, 2015 an unknown hacker publicly announced on Twitter that he had breached the internal network of Hacking Team – an Italian pentesting company known to purchase 0-day exploits and produce their own trojans. The hacker proceeded to leak archives of internal Hacking Team tools and communications. A number of tools and previously unknown exploits were discovered in the trove of data posted online.

In the attached paper we will focus on two exploits which at the time of discovery in the Hacking Team archives were unpatched. The two 0-days in question targeted Adobe Flash and were subsequently labeled CVE-2015-5119 and CVE-2015-5122.

The goal of this research is to demonstrate how quickly these exploits spread and were used by multiple independent cyber espionage operators. Via the evidence presented within this paper we will demonstrate that at least two different exploit kits, or generators, were

constructed by an unknown entity and shared amongst multiple operators believed to be located in China. We believe the following is a clear example of yet another 'digital quartermaster' of cyber espionage tools.

To read the full report click **here**.

Download the IOCs **here**.

Threat Intelligence

« Back to News & Insights

Recent Articles

Celebrating Milestones (European CERT/CSIRT Report Coverage)

FEBRUARY 23, 2020

Celebrating a particularly significant long term milestone - our 107th National CERT/CSIRT recently signed up for Shadowserver's... **Read more »**

Dridex update: The wheels of international Law Enforcement keep on turning

DECEMBER 5, 2019

The Dridex botnet was sinkholed in October 2015 and the infected victims remediated via Shadowserver's free daily network... **Read more »**

Beyond the SISSDEN event horizon

OCTOBER 1, 2019

Between May 2016 and April 2019, The Shadowserver Foundation participated in the SISSDEN EU Horizon 2020 project. The main goal...
Read more »

Of Vacations and Armageddon

JUNE 3, 2019

2019-06-02 - 0820 UTC-7 - It seems that the power company "accidentally" turned off all the power to the building where our data... **Read more »**

Search