FBI FLASH

FBI LIAISON ALERT SYSTEM
#R-000029-MW

(U) The following information was obtained through FBI investigation and is provided in conjunction with the FBI's statutory requirement to conduct victim notification as outlined in **42 USC § 10607**.

SUMMARY

(U) On May 19, 2014, the FBI announced a worldwide operation against those individuals who created and purchased malware known as Blackshades. Blackshades products were offered on their website which offered several products ranging in price from $5 to $40 U.S. Dollars. These products include Blackshades Remote Access Tool (RAT), Blackshades Password Recovery, Blackshades Stealth, Blackshades Fusion, Blackshades Commander, Blackshades Crypter, and Blackshades Virtual Private Network (VPN). The most popular product was the Blackshades RAT. The command and control aspect of the malware included a graphical user interface to manage the infected computers. The malware was custom-tailored to the specifications selected by the user, then compiled on the Blackshades server, and delivered to the user's computer.

TECHNICAL DETAILS

(U) **How Blackshades Connects to Victim's Computers:**

(U) In order for a connection to be established, the malware on a victim computer must know the IP address and listening port on the command and control computer. Given that many users have a dynamic IP address controlled and assigned by their Internet Service Provider, the malware is programmed to call to a unique domain names created by the Blackshades user. The Blackshades user associated this name with their IP address using any domain hosting service of their choice. In this manner, when the malware calls to the established domain, standard DNS protocols will route the malware to the Blackshades user's IP address.

(U) The FBI is providing approximately 13,600 domains used by Blackshades users, which have been observed receiving status updates or have participated in previous attacks. These URLs are located within the United States and worldwide. The FBI is distributing these indicators to enable identification of Blackshades infections on their networks. The FBI has **high confidence** that these indicators were involved in past Blackshades related activity. The FBI recommends that your organization help victims identify and remove the malicious code.

Notes on Domain List: Computers infected with Blackshades may make DNS queries for these domains and attempt to connect to the corresponding IP addresses (usually on destination port 3080, 3333 or 4444). Disclaimer: these domains may be used for legit traffic.

POINT OF CONTACT

Please contact the FBI with any questions related to this FLASH report at either your local CTF or **FBI CYWATCH: Email: cywatch@ic.fbi.gov or Voice: +1-855-292-3937**