FBI Cyber Division

Private Industry Notification

DATE: 05/19/2014

PIN #: 140519-001

(U) FBI led takedown of "Blackshades Remote Access Tool" purchasers, developers

(U) General Observations

(U) On 13 May 2014, FBI NY initiated a coordinated takedown focusing on individuals who purchased the Blackshades malware. Field offices across the United States, as well as foreign partners, engaged in subject interviews, searches, hardware seizures, and arrests. The FBI seized the primary domain utilized to purchase Blackshades products.

(U) Impact

(U) Blackshades has several products marketed for $5 to $40 USD, most of which are malware. 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 and versatile product sold by Blackshades is the Blackshades RAT. These are purchased as "off the shelf" products with a wide variety of features that allow a cyber criminal to use as they desire. Once the victim computer is infected, common uses for Blackshades include: access to victims' computers; theft of passwords and credentials; key-logging ability; and Distributed Denial of Service attacks.

(U) Prior to the coordinated actions, two subjects associated with the Blackshades organization were arrested. Alex Yucel was identified as the developer of the Blackshades malware. Yucel not only wrote software code behind the malware, but also was responsible for improvements and updates to the malware and control of the Blackshades server. Yucel was arrested by Moldovan authorities in November 2013 and is currently awaiting extradition to the United States. Michael Hogue, a known seller and "customer service advisor" in the Blackshades organization was arrested in June 2012 and subsequently pled guilty to the charges against him.

(U) Administrative Note: Law Enforcement Response

The FBI Cyber Division and the FBI New York Field Office express gratitude for the exceptional coordination and assistance demonstrated throughout this highly successful operation. Without the assistance of the European Union's Judicial Cooperation Unit, the European Cyber Crimes Centre/EUROPOL, numerous foreign partnerships, and dedicated private industry partners, this takedown would have been much less successful.