CALIFORNIA STATE THREAT ASSESSMENT CENTER

PRIMER – CYBER SECURITY

THE STAC PRIMER PROVIDES HISTORIC OR BIOGRAPHIC INFORMATION WITH ONLY LIMITED COMMENT OR ANALYSIS ON A SPECIFIC SUBJECT.

PUB DATE: 20150305
DOI: 20150220
STAC-20150301

(U) DarkComet: Security Surveillance Tool Turned Malicious Remote Access Trojan

(U) SUMMARY: DarkComet—a network administration tool formerly used in security and law enforcement applications for surveillance purposes—has been employed by malicious cyber actors as a Remote Access Trojan[a] (RAT) with Distributed Denial of Service (DDoS) capabilities. *Hackers who infect a victim with DarkComet have full access to files, their computer system, and network. Notably, DarkComet provides the ability for malicious users to control a victim's webcam clandestinely, which is often used to capture pictures for illicit purposes, such as blackmail or espionage. According to reliable open source news and a recognized non-profit organization, Syria allegedly used DarkComet to target political dissidents circa 2012.*[1,2]

(U) Affected Systems

(U) DarkComet has been successfully ported across many Operating Systems (OS), including all versions of Windows, most Apple[USPER] OS-X, and Linux distributions.

(U) Exploitation Vectors

(U) DarkComet users generally attack through social media drive by downloads[b], or through trojans attached to pirated programs.

- (U) DarkComet is widely available in online hacker circles, either for free or a set fee. Many of these versions are themselves infected with RATs, thus giving another hacker access to the systems of the hacker who downloaded the program.
- (U) For drive by downloads, and social media exploitation, victims are usually directed to a seemingly trustworthy page, and told to download a new version of an Adobe[USPER] product, which is already infected.

(U) Protective/Prevention Measures

(U) DarkComet has enough of a history that most updated anti-virus/anti-malware software can detect most versions of the program, and maintaining up-to-date patches is critical to protecting a system from DarkComet. Furthermore, users should be cognizant of the danger posed by drive by downloads and accepting executable files from websites.

(U) Mitigation Measures

(U) DarkComet generally in most cases can be easily removed via an updated anti-virus program.

(U//FOUO) Analysis

(U//FOUO) We assess RATs, such as DarkComet, are probably among the most dangerous forms of malware because of their ability to give a hacker complete system control.

(U) BlackShades RAT, DarkComet Predecessor: Prior to DarkComet, one of the most commonly seen RATs was BlackShades, a RAT that was created for cyber-crime purposes. In 2012, an international crackdown on the malware and malicious users was led by the FBI and dubbed "Operation Card Shop." Prior to this crackdown, BlackShades was exceedingly common, having infected over a half million computers. Hackers likely will seek a new tool to replace BlackShades.[3]

a. (U) Remote access trojans are malicious programs that run invisibly on host Personal Computers (PCs) and permit an intruder remote access and control. On a basic level, many RATs mimic the functionality of legitimate remote control programs but are designed specifically for stealth installation and operation.

b. (U) A "drive by download" is a specialized form of attack wherein a victim's Internet browser is hijacked simply by visiting the site. There is no accepting of a download or other action by the victim.

Form # 91167e4d-c4d3-488a-be0b-ada2098e0cbe

(U) ADMINISTRATIVE NOTE

(U) Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. http://www.us-cert.gov/tlp/

(U) For comments or questions related to the content or dissemination of this document, please contact the STAC at (916) 874-1100 or STAC@caloes.ca.gov.

(U) TRACKED BY

(U) HSEC-8.2.2, HSEC-8.2.3, HSEC-8.6.1

(U) FEEDBACK

(U) The STAC encourages your feedback using the survey found at https://www.surveymonkey.com/s/YK3X8TL

(U) ENDNOTES

---

1. (U) Internet site; Pierluigi Paganini; *Security Affairs;* "Syria, Uncomfortable Assumptions on the Control of Dissidents;" 18 May 2012; http://securityaffairs.co/wordpress/5419/intelligence/syriauncomfortable-assumptions-on-the-control-of-dissidents.html; accessed on 27 January 2015; Security Affairs is a recognized technology security site.

2. (U) Internet Site; Eva Galperin and Morgan Marquis-Boire; *Electronic Frontier Foundation;* "Pro-Syrian Government Hackers Target Activists With Fake Anti-Hacking Tool;" 15 August 2012; https://www.eff.org/deeplinks/2012/08/syrian-malware-post; accessed on 27 January 2015; The Electronic Frontier Foundation is the preeminent nonprofit organization in regards to electronic freedoms and online surveillance monitoring.

3. (U) Internet Site; Larry Neiumeister; *phys.org;* FBI: "BlackShades infected half-million computers" 19 May 2014; http://phys.org/news/2014-05-raids-blackshades-hackers.html; accessed 19 February 2015; phys.org is a news site focusing on science and technology