IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	)	
	)	
Plaintiff,	)	Civil Action No. 14-0685
	)	
v.	)	
	)	
EVGENIY MIKHAILOVICH BOGACHEV, et al.	)	
	)	
	)	
Defendants.	)	

STATUS REPORT

The United States of America, by and through its attorneys David J. Hickton, United States Attorney for the Western District of Pennsylvania and Leslie R. Caldwell, Assistant Attorney General, respectfully submits this status report.

I. The Defendants

Although the Defendants have been properly served with the pleadings filed in this case as well as the Temporary Restraining Order ("TRO") and Preliminary Injunction ("PI") entered by this Court, the Defendants have failed to answer or otherwise respond to the Government's Complaint. The Government has not been contacted by the Defendants or any attorney representing the Defendants. As a result, the Government has filed herewith a motion requesting that the Clerk declare the Defendants in default pursuant to Fed. R. Civ. P. 55(a). Once a default is entered, the Government will move for a default judgment pursuant to Fed. R. Civ. P. 55(b).

II. The Technical Disruption of Gameover Zeus and Cryptolocker

During the PI hearing on June 3, 2014, the Government reported that the technical measures and injunctive relief authorized by the TRO and PI – combined with action taken by law enforcement partners abroad – had successfully neutralized both Gameover Zeus ("GOZ")

and Cryptolocker. Specifically, the Government reported that the computers in the GOZ botnet had been liberated from the Defendants and were now communicating exclusively with the substitute server created pursuant to this Court's Orders. The Government also reported that the Cryptolocker infrastructure had been dismantled, and that the Cryptolocker malware was no longer capable of encrypting newly infected computers.

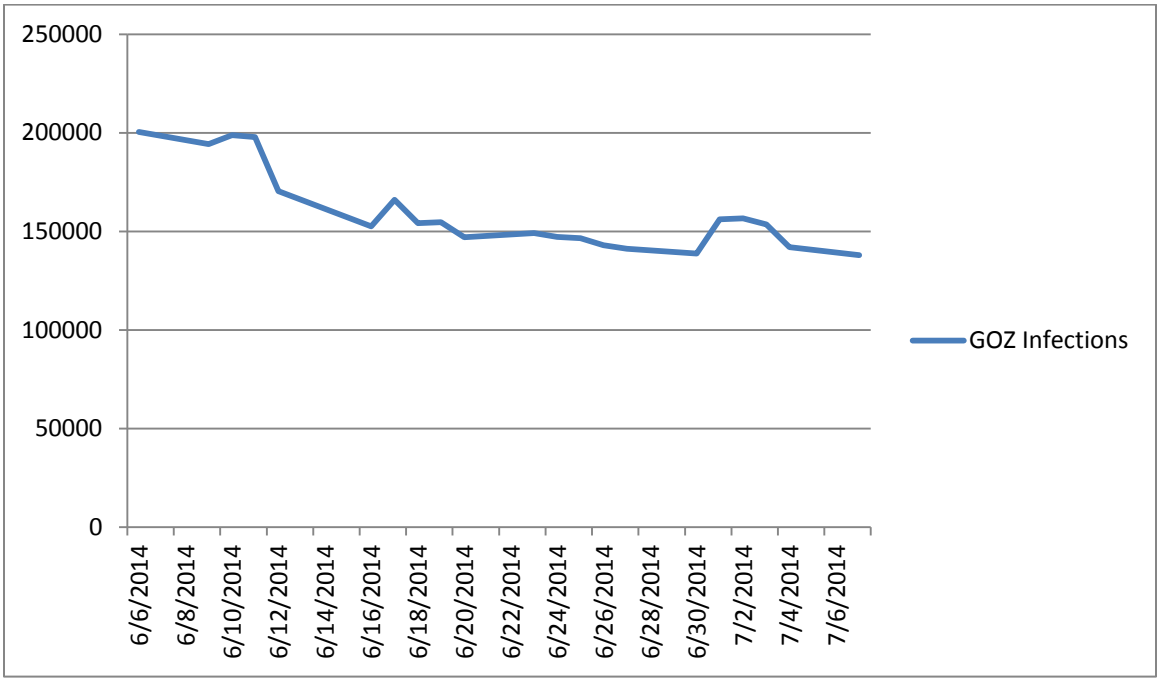
As of today, both GOZ and Cryptolocker remain neutralized. Moreover, as detailed below, significant progress has been made in remediating computers infected with GOZ.

A. GOZ

Analysis to date indicates that all or nearly all of the active computers in the GOZ network are communicating exclusively with the substitute server established pursuant to this Court's Orders. Traffic data from the substitute server shows that a total of 200,407 bots were communicating with the server on June 6, 2014.[1] As of July 7, 2014, the total number of bots had fallen to 137,863 – a reduction of more than 31%. This decline in infections is attributable to successful remediation efforts undertaken by Internet Service Providers, as well as direct remediation undertaken by victims who downloaded the malware removal tools supplied on the Government's remediation website, *www.us-cert.gov/gameoverzeus*. The chart below shows the

[1] Measuring the number of GOZ-infected computers communicating with the substitute server has proved complex. Each computer in the GOZ botnet is assigned a unique number or "bot ID". The Government believes that tallying unique bot IDs is the best method of counting infected bots. However, the process is not perfect. Third parties, including security researchers, posing as bots in the network are generating numerous fake bot IDs, which must be sorted out of the total count. The Government believes that the numbers supplied in this Status Report reflect as accurately as is possible the true number of infected victim computers.

steady progress made to date in remediating GOZ infections.



B. Cryptolocker

Government testing of Cryptolocker malware samples has confirmed that Cryptolocker is no longer able to encrypt newly infected computers and, as a result, is not currently a threat. Cryptolocker must communicate with its command and control infrastructure in order to encrypt newly infected computers. As of today, the injunctive relief ordered in the TRO and PI has knocked all of Cryptolocker's infrastructure offline, and has thereby neutralized Cryptolocker.

III. Conclusion

The technical disruption of Gameover Zeus and Cryptolocker continues to function as designed, and both GOZ and Cryptolocker remain neutralized. The Government will continue to work with private sector representatives both domestically and abroad to encourage them to remediate infected computers. To ensure that the Court is kept up to date on these remediation

efforts, and any other developments, the Government proposes to file another status report on August 15, 2014.

Dated: July 11, 2014

Respectfully submitted,

DAVID J. HICKTON
United States Attorney

By: /s/ Michael A. Comber
MICHAEL COMBER
Assistant U.S. Attorney
Western District of Pennsylvania
U.S. Post Office & Courthouse
700 Grant Street, Suite 4000
Pittsburgh, PA 15219
(412) 894-7485 Phone
(412) 644-6995 Fax
PA ID No. 81951
Michael.Comber@usdoj.gov

LESLIE R. CALDWELL
Assistant Attorney General

By: /s/ Ethan Arenson .
ETHAN ARENSON
DAVID AARON
Trial Attorneys
Computer Crime and Intellectual Property Section
1301 New York Avenue, NW
Washington, DC 20530
(202) 514-1026 Phone
(202) 514-6113 Fax
DC Bar No. 473296 (Arenson)
NY Bar No. 3949955 (Aaron)
Ethan.Arenson@usdoj.gov
David.Aaron@usdoj.gov