National Terrorism Advisory System

www.dhs.gov/NTAS

24x7 Watch Desk: +1(317)227-6690
http://www.REN-I5AC.net
IPPQ-RENI5ACNET
SOC at ren-isac dot net

Commercial, government, and private sector information sharing relationships.

The REN-I5AC mission is to aid and promote other security operational production and

Content © 2008-2012, Research and Education Networking Information Sharing and Analysis Center

All rights reserved.
address: dprt = destination port  
    key: src = source port, srcd = protocol, dsrcd = destination  
    p2p | 147.144.13.119 | 2012-11-30T00:00:00Z:017 | 20404  
    tsrc = destination address | timestamp in UTC | sprt  
    z = Zues.  
    t = Trojan Zeus, a variant known as Gameover Zeus or P2P  
    host(s): have been identified as likely compromised with  
    Greetings,  
    On Mon, Dec 3, 2012 12:35:27 AM, soc@ren-isac.net wrote:  
    Incident:  
    Send mail to abuse-mgmt@cenic.org for concerns or questions related to the handling of this  

http://www.cenic.org/cgi-bin/arpmlf  
www.cenic.org  
714-220-3494 or 714-220-5177  
CENIC Network Operations  
Thank you,  
Please investigate the alleged event and respond directly to the complainant: soc@ren-.  
Span of suspicious activity appears to have originated from your IP address 147.144.13.119.  
In the attached message below, Research and Education Networking ISAC has reported that  
Dear City College of San Francisco,  

<< << Over Do We RT! abuse@cenic.org 12/3/2012 3:23 PM >> >>
[1] The Lifecycle of Peer-to-Peer (Gameover) ZeuS

[2] Is created using a Trojan-building toolkit. Trojan

randomly chooses ports between 1,000 and 30,000. [1]

5,000 and UDP on TCP and UDP on

< peer list is requested. Communication with peers occurs over TCP and UDP on

< a set of hard-coded peers in which communication takes priority. Updates and a

< list of peer-to-peer (P2P) networks to communicate. Communication starts with

< P2P ZeuS is like all other variants of the ZeuS Trojan except that

<

Regarding P2P ZeuS:

http://www.jenn-scown.com
24XX Watch Desk: +1(317)278-6650, sec@ven-secure.net
Research and Education Networking IASC

<

This information provided useful.

< Meaning back from you regarding action on this incident and how, if at all,

< community with network security matters would greatly appreciate

< In order for the IASC to learn how we can best aid the education

< Additional information regarding P2P ZeuS is provided below.

< If you feel you've received this report in error, please let us know.

<

<

<

<

<

<

<

<

<

<

<

<

- Format data in an automated processing with your Incident Tracking System.
- OIDEF: For in the attached file. If you have questions about using the OIDEF.
- Attachments: The incident data presented above is also provided in
  - Attached attacks on institutional online banking
  - http://www.zeus-secure.com/research/threats/zeus/threat-zews
  - Zeus Banking Trojan Report
  - ZeuS King of the P2P command


http://www.zeus-secure.com/y-door/y-door-spy-zeus-zbot.shim
http://www.spy-w32zbot.com
http://www.spy-w32zbot.com
http://www.spy-w32zbot.com
http://www.spy-w32zbot.com


Additional Information:
011016-3514-99
14039/9/02010