Network Flow Data Analysis Using Graph Pattern Search

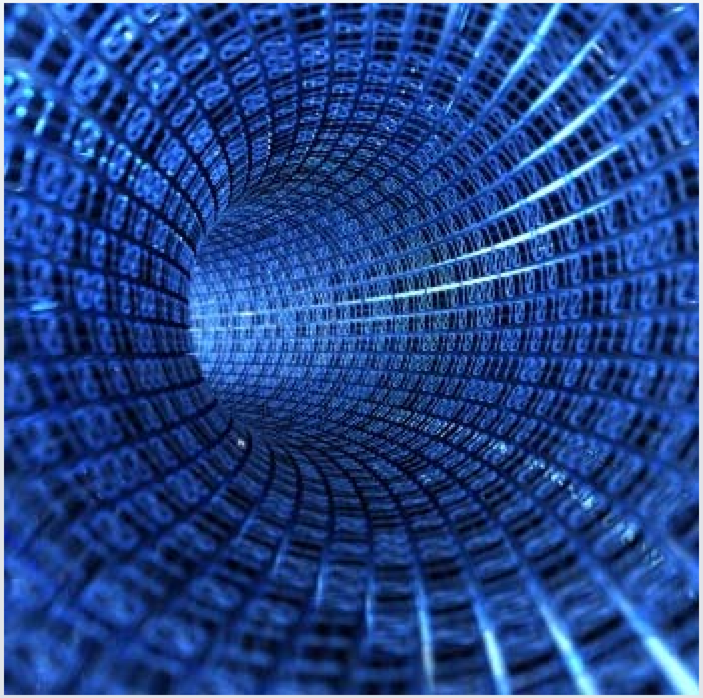
Josh Goldfarb

FloCon 2011

Salt Lake City, UT

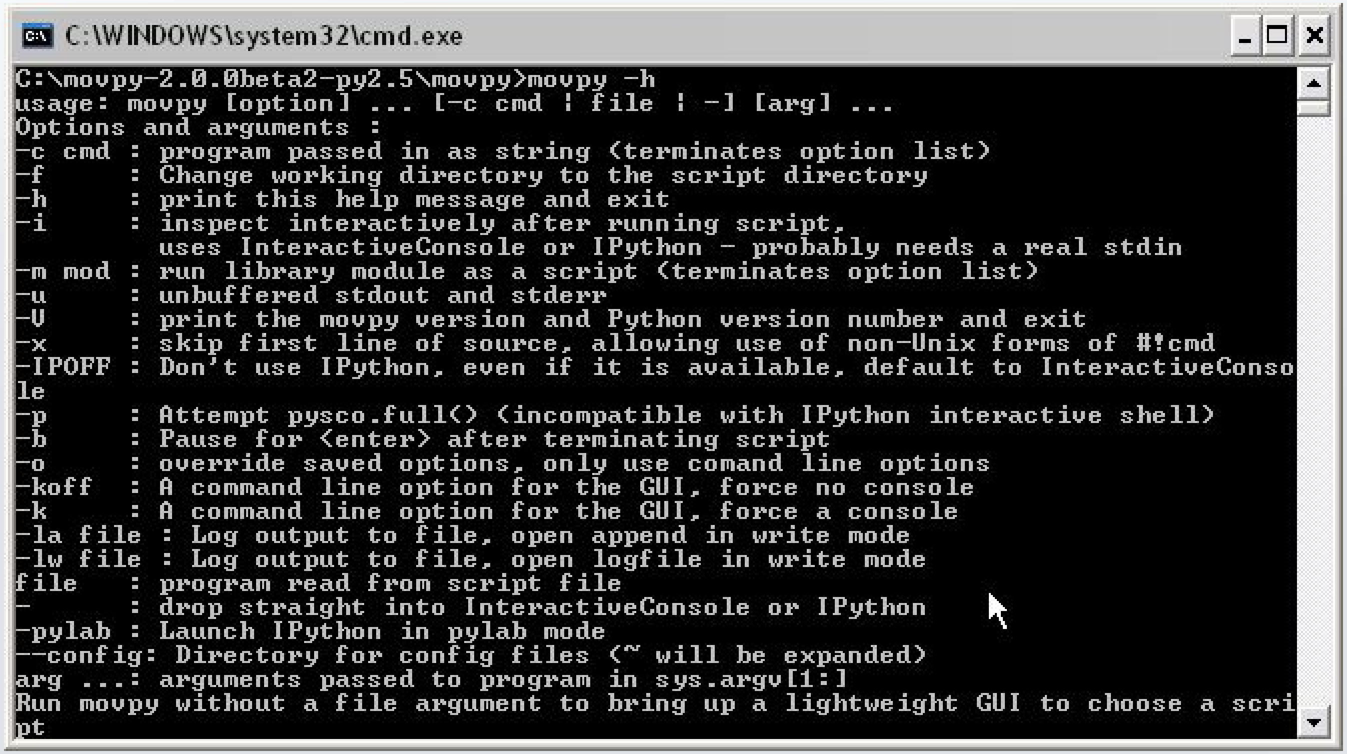
21st CENTURY TECHNOLOGIES

Problem



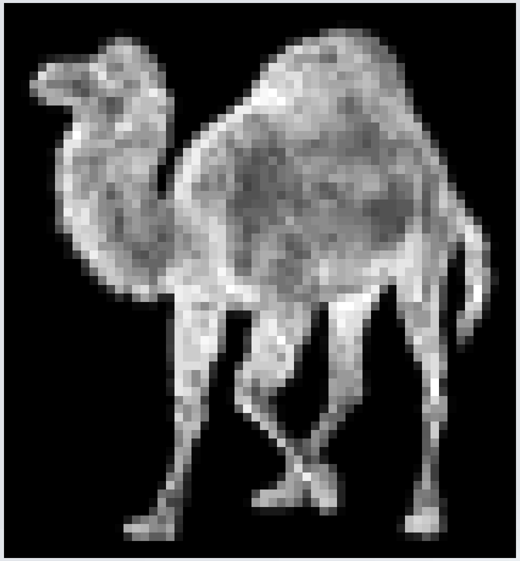
Problem Solvers

Most Tools

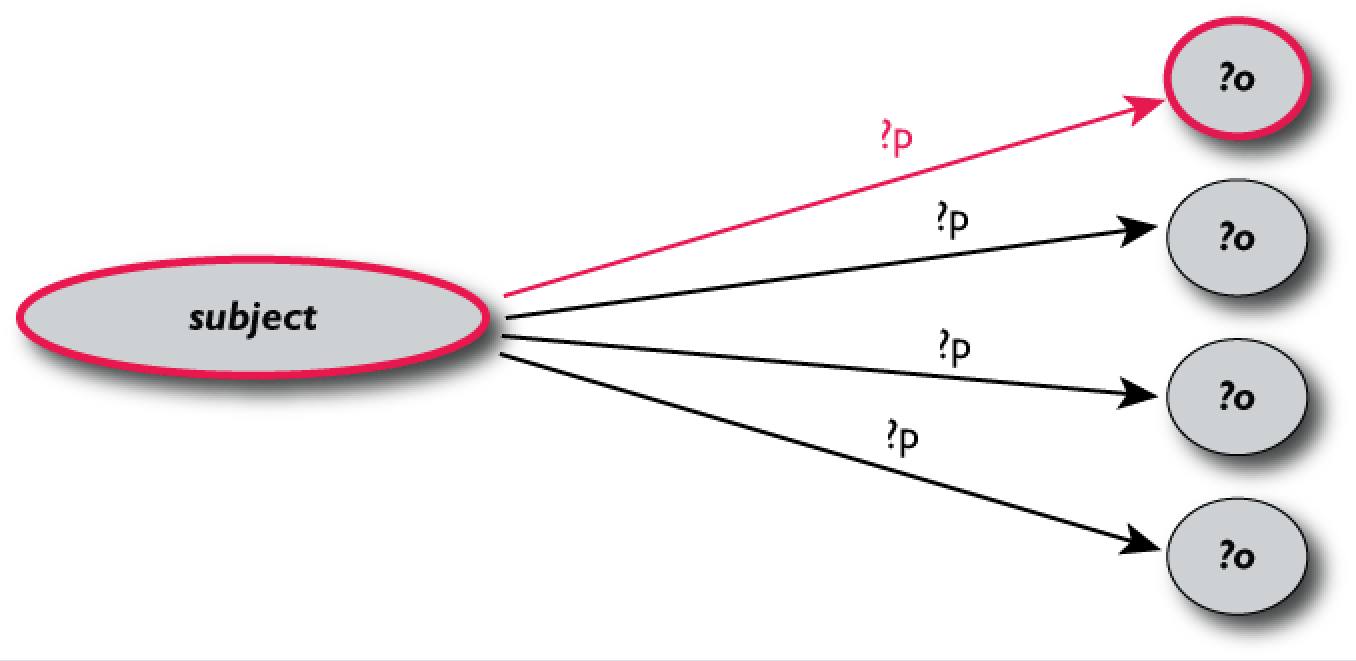


```
C:\movpy-2.0.0beta2-py2.5\movpy>movpy -h
usage: movpy [option] ... [-c cmd | file | -] [arg] ...
Options and arguments :
-c cmd : program passed in as string (terminates option list)
-f     : Change working directory to the script directory
-h     : print this help message and exit
-i     : inspect interactively after running script,
         uses InteractiveConsole or IPython - probably needs a real stdin
-m mod : run library module as a script (terminates option list)
-u     : unbuffered stdout and stderr
-V     : print the movpy version and Python version number and exit
-x     : skip first line of source, allowing use of non-Unix forms of #!cmd
-IPOFF : Don't use IPython, even if it is available, default to InteractiveConso
le
-p     : Attempt pysco.full() (incompatible with IPython interactive shell)
-b     : Pause for <enter> after terminating script
-o     : override saved options, only use comand line options
-koff  : A command line option for the GUI, force no console
-k     : A command line option for the GUI, force a console
-la file : Log output to file, open append in write mode
-lw file : Log output to file, open logfile in write mode
file   : program read from script file
-      : drop straight into InteractiveConsole or IPython
-pylab : Launch IPython in pylab mode
--config: Directory for config files (~ will be expanded)
arg ...: arguments passed to program in sys.argv[1:]
Run movpy without a file argument to bring up a lightweight GUI to choose a scri
pt
```

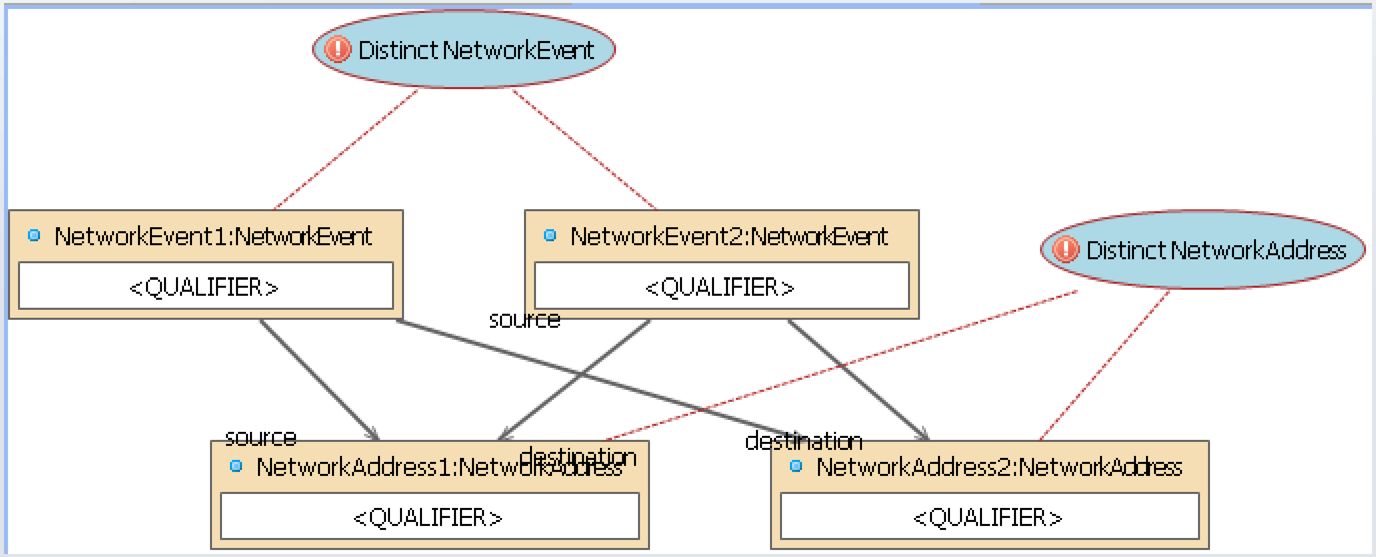
Or Perhaps



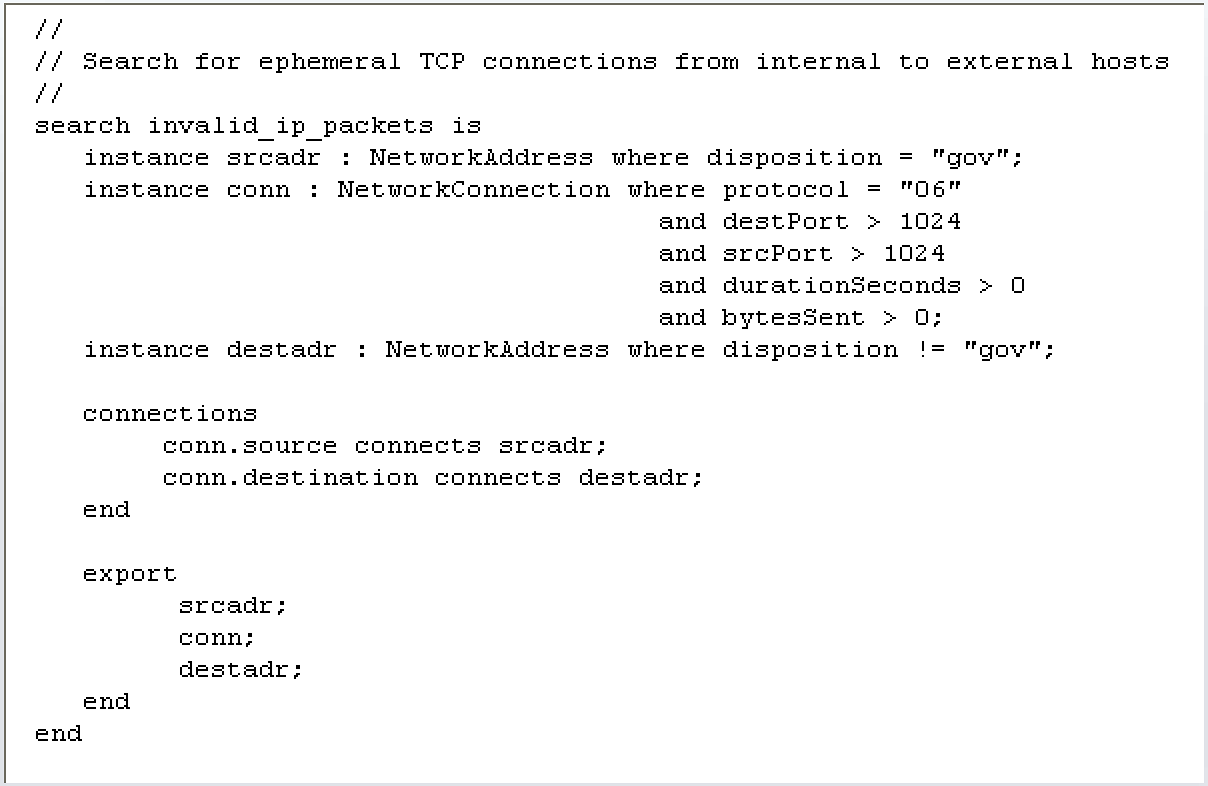
Another Option



Build Pattern

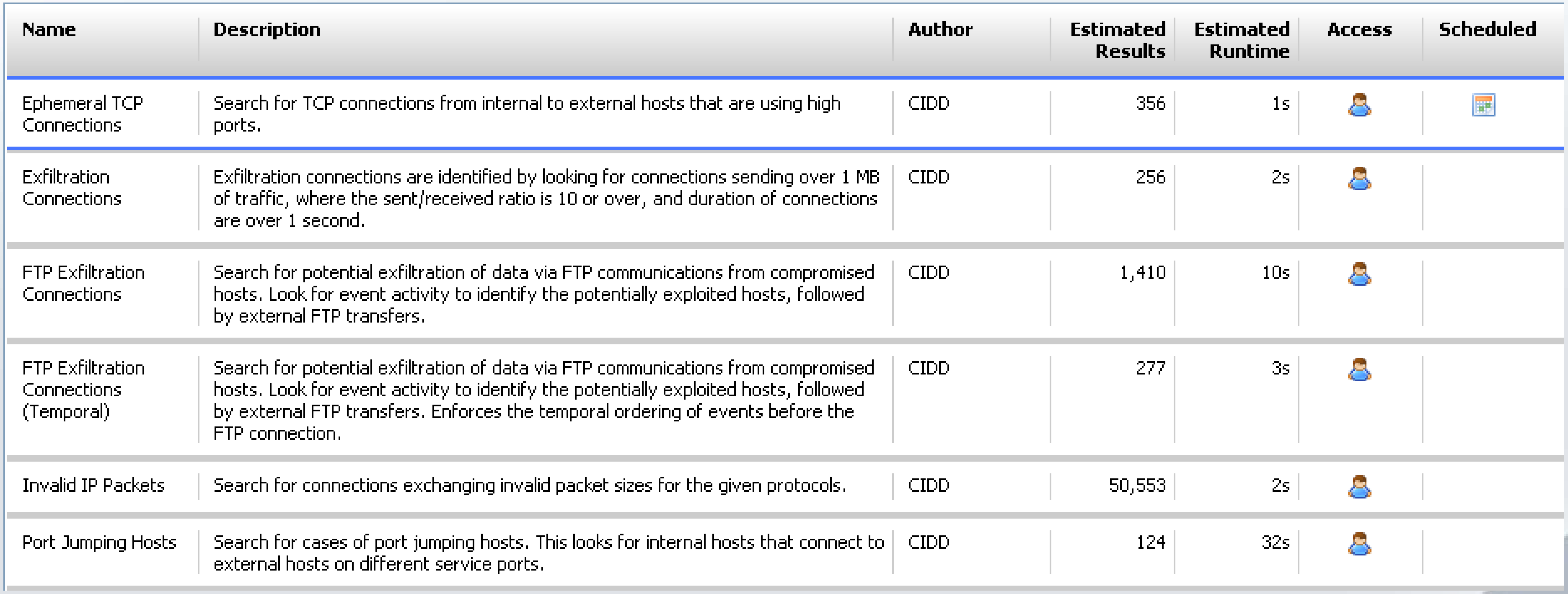


Admire Pattern



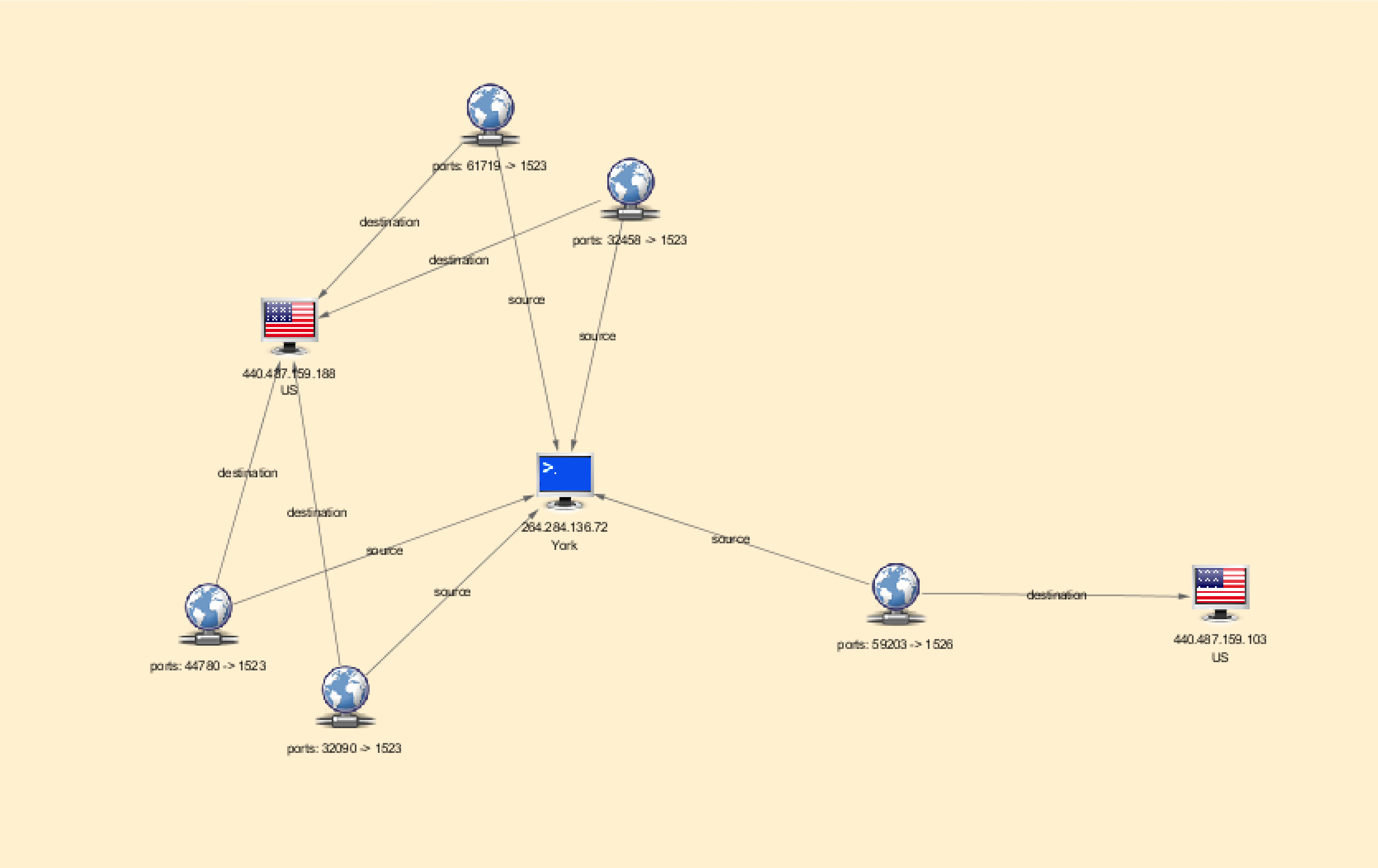
```
//
// Search for ephemeral TCP connections from internal to external hosts
//
search invalid_ip_packets is
   instance srcadr : NetworkAddress where disposition = "gov";
   instance conn : NetworkConnection where protocol = "06"
                                       and destPort > 1024
                                       and srcPort > 1024
                                       and durationSeconds > 0
                                       and bytesSent > 0;
   instance destadr : NetworkAddress where disposition != "gov";

   connections
        conn.source connects srcadr;
        conn.destination connects destadr;
   end

   export
         srcadr;
         conn;
         destadr;
   end
end
```

Execute Pattern

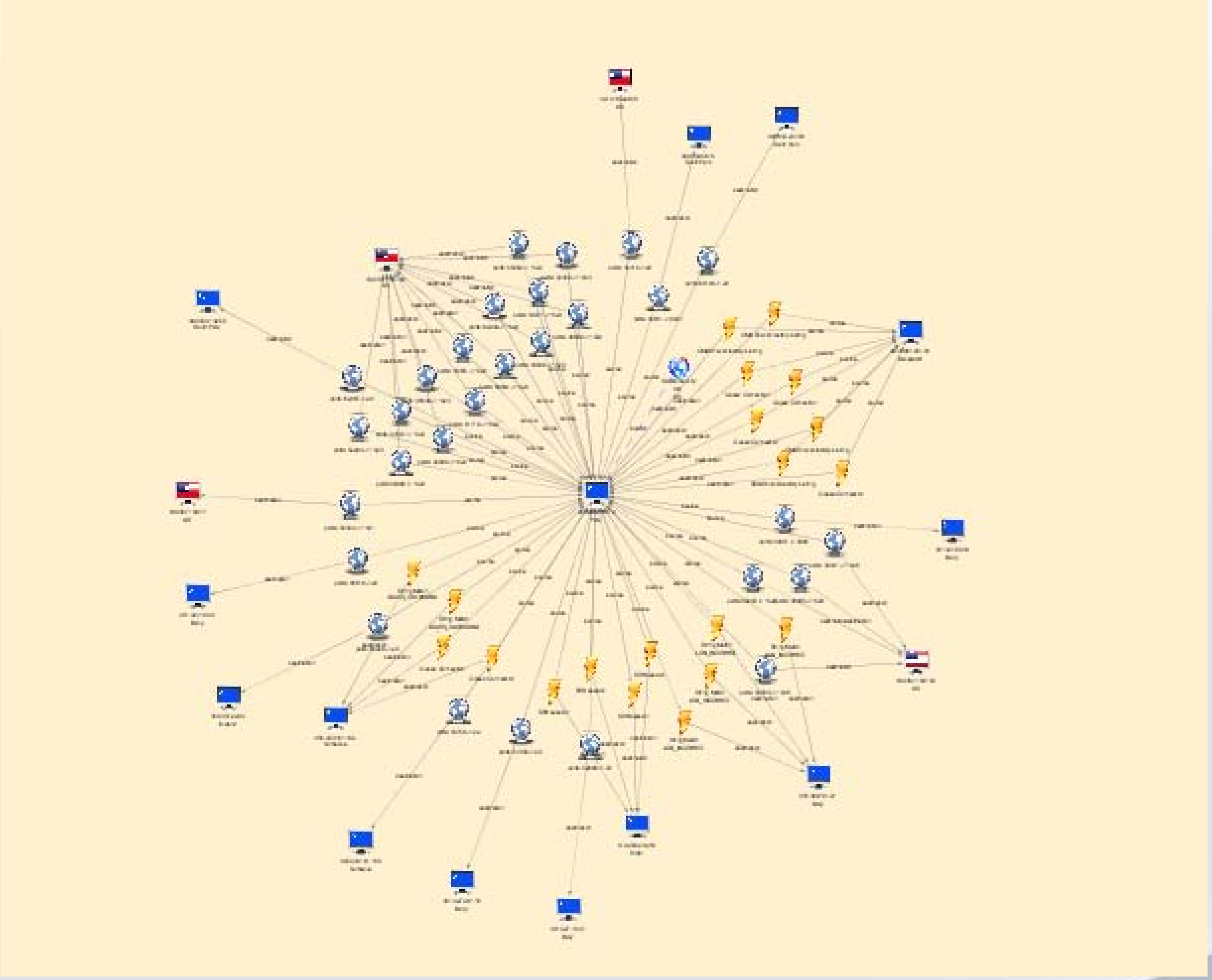


Name	Description	Author	Estimated Results	Estimated Runtime	Access	Scheduled
Ephemeral TCP Connections	Search for TCP connections from internal to external hosts that are using high ports.	CIDD	356	1s	👤	📅
Exfiltration Connections	Exfiltration connections are identified by looking for connections sending over 1 MB of traffic, where the sent/received ratio is 10 or over, and duration of connections are over 1 second.	CIDD	256	2s	👤	
FTP Exfiltration Connections	Search for potential exfiltration of data via FTP communications from compromised hosts. Look for event activity to identify the potentially exploited hosts, followed by external FTP transfers.	CIDD	1,410	10s	👤	
FTP Exfiltration Connections (Temporal)	Search for potential exfiltration of data via FTP communications from compromised hosts. Look for event activity to identify the potentially exploited hosts, followed by external FTP transfers. Enforces the temporal ordering of events before the FTP connection.	CIDD	277	3s	👤	
Invalid IP Packets	Search for connections exchanging invalid packet sizes for the given protocols.	CIDD	50,553	2s	👤	
Port Jumping Hosts	Search for cases of port jumping hosts. This looks for internal hosts that connect to external hosts on different service ports.	CIDD	124	32s	👤	

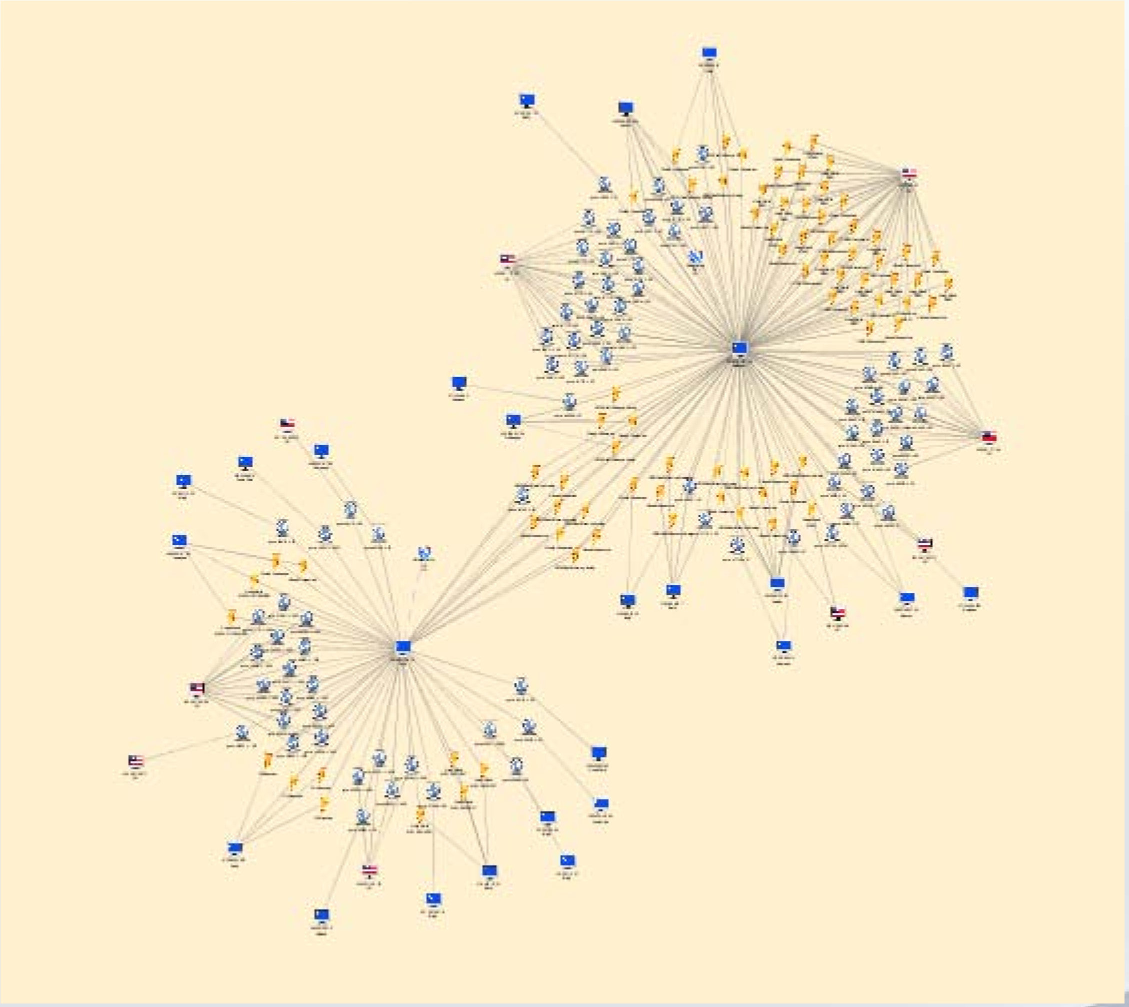
View Results



Pivot



Pivot Again



Report, Study, Revise, and Preserve

Be Happy

Questions?

Josh Goldfarb

Director, Cyber Analysis Solutions

21st Century Technologies, Inc.

jgoldfarb@21technologies.com