LA-UR- 11-02428

Approved for public release;
distribution is unlimited.

Title: Cyber Security R&D [~~Research and Development~~]

Author(s): Ahmad Douglas

Intended for: 2011 Federal Labs Consortium (A Conference)
Nashville, Tennessee USA
2-5 May 2011

Los Alamos
NATIONAL LABORATORY
EST. 1943

Los Alamos National Laboratory, an affirmative action/equal opportunity employer, is operated by the Los Alamos National Security, LLC for the National Nuclear Security Administration of the U.S. Department of Energy under contract DE-AC52-06NA25396. By acceptance of this article, the publisher recognizes that the U.S. Government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or to allow others to do so, for U.S. Government purposes. Los Alamos National Laboratory requests that the publisher identify this article as work performed under the auspices of the U.S. Department of Energy. Los Alamos National Laboratory strongly supports academic freedom and a researcher's right to publish; as an institution, however, the Laboratory does not endorse the viewpoint of a publication or guarantee its technical correctness.

Cyber Security R&D
Ahmad Douglas

Presentation Abstract for Classification Review

This presentation is intended for a conference, the 2011 Federal Labs Consortium in Nashville, Tennessee from May 2-5, 2011. The purpose of this presentation is to convey Los Alamos as a key player in the cyber (computer) security R&D space, give several examples of open science-based, unclassified contributions we are making to the field, and generate interest in partnerships with industry.

I'll talk about our three goals for research in this area being:

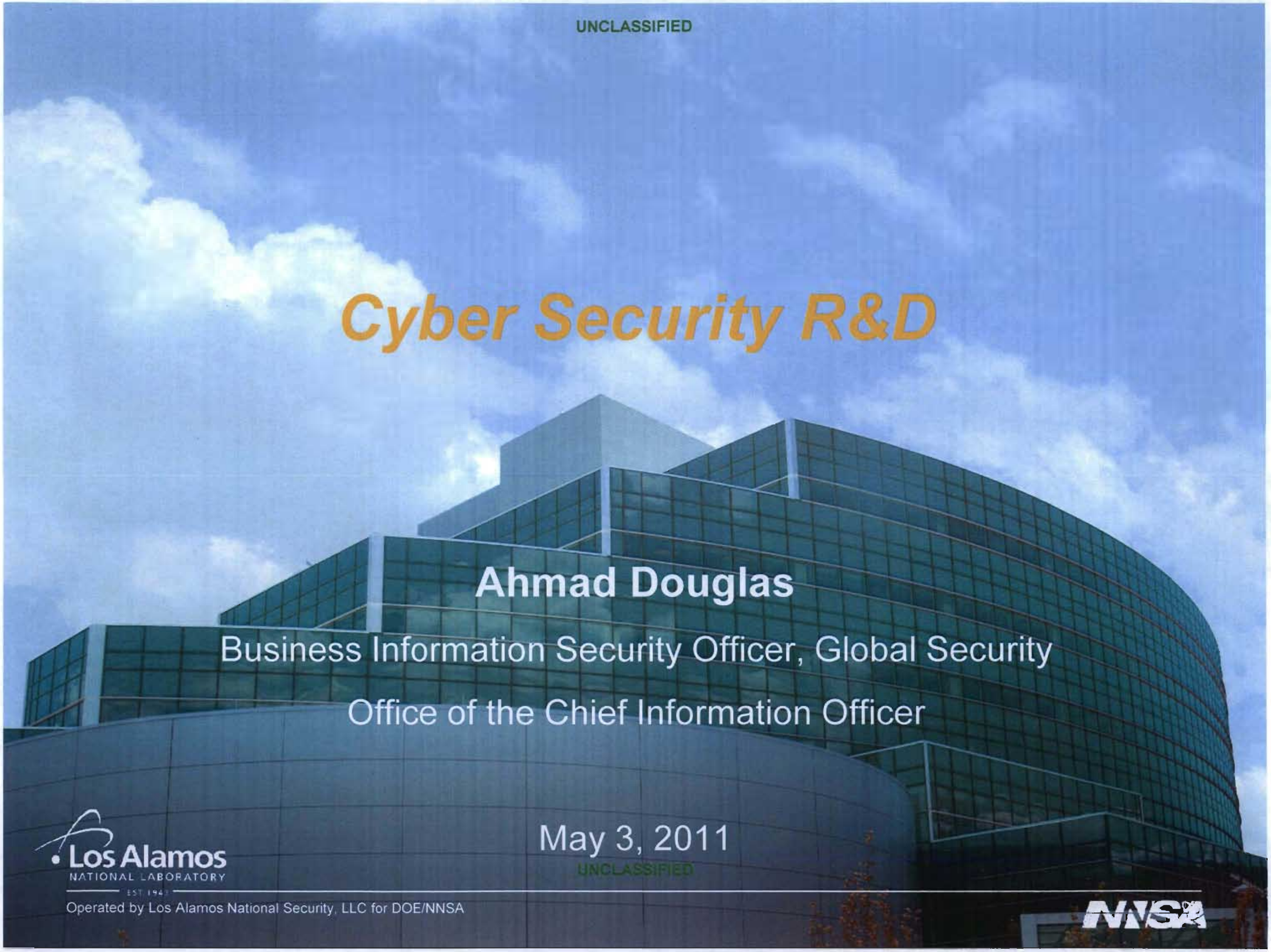
- Avoid *cyber surprise* – this means we should avoid being completely outflanked by an adversary in the cyber security arena;
- Mitigate the fundamental asymmetry – that is to say, the attackers (offense) generally have strong incentives and no consequences for attacking. We develop technologies to change that landscape by making attack more costly (in terms of resources) and increasing the chance of getting caught;
- Improve detection, deterrence, and response capabilities – these are the operational tools that allow us to mitigate the fundamental asymmetry, as described immediately prior.

I will discuss the strong collaborative nature of our multiprogram laboratory, explaining how our rich strengths in a number of disciplines play off of each other to create a cyber security center of excellence.

I will discuss in very general terms why organizations should be concerned about insider threats and unmanaged technology (non-company owned thumb drives and computers) coming on site. I will then speak to some of the unclassified IT research we have done to improve our own operations.

I will then present several examples of completely unclassified, open science-based computer science research projects we have been working on to countermand the cyber threat. These include MassAV (an anti-virus tool), statistical anomaly detection, and honey wrappers (a tool for confusing someone attacking your network). I'll also discuss two response tools that are also completely unclassified, namely automated malware analysis, and a model of lateral movement of hackers inside a network.

I will end the presentation with a brief pitch about Los Alamos being open to cooperative research and development agreements (CRADAs) with industry, and encourage them to contact our Technology Transfer division if they are interest in pursuing one.



Cyber Security R&D

Ahmad Douglas

Business Information Security Officer, Global Security

Office of the Chief Information Officer

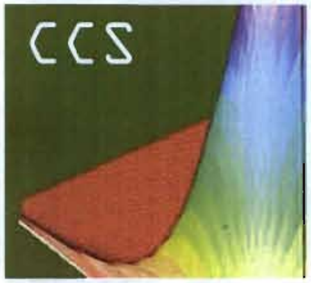
May 3, 2011

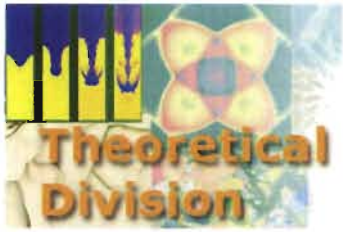
Our Approach to Cyber Security

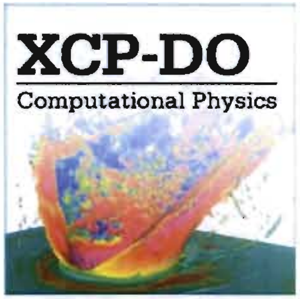
- **Evolution**
  - Operational excellence
  - Continual process improvement

- **Revolution**
  - Rich heritage of innovation in weapons and national security science
  - Cyber security is multidisciplinary → maps well to a multi-program Laboratory
  - Overarching program goals
    - Avoid cyber surprise
    - Mitigate the fundamental asymmetry
    - Improve detection, deterrence, and response capabilities

A Culture of Collaboration







Avoid Cyber Surprise

- 0day research
- Countering the insider threat
- Setting realistic expectations

Mitigate the Fundamental Asymmetry

Offense

- “There Exists”
- Low risk
- Low resource requirements

Defense

- “For All”
- Moderate to high risk
- High resource requirements

Improve Detection and Deterrence Capabilities

MassAV

Search

MassAV Statistics

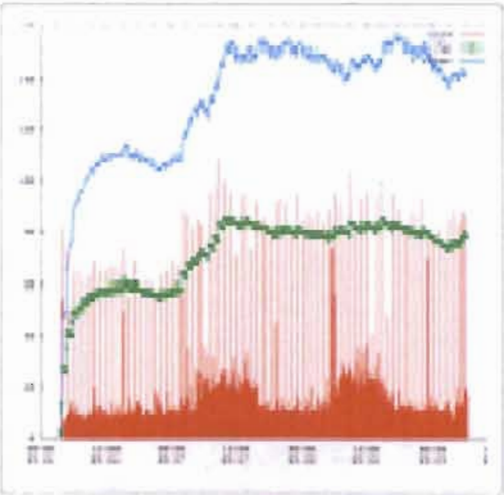
Last 24 Hours

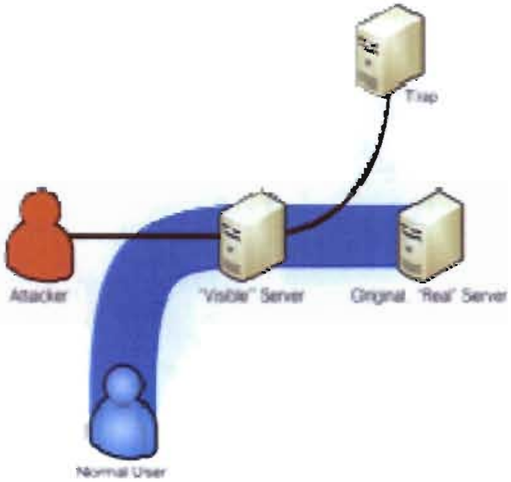
All Time

Service Load

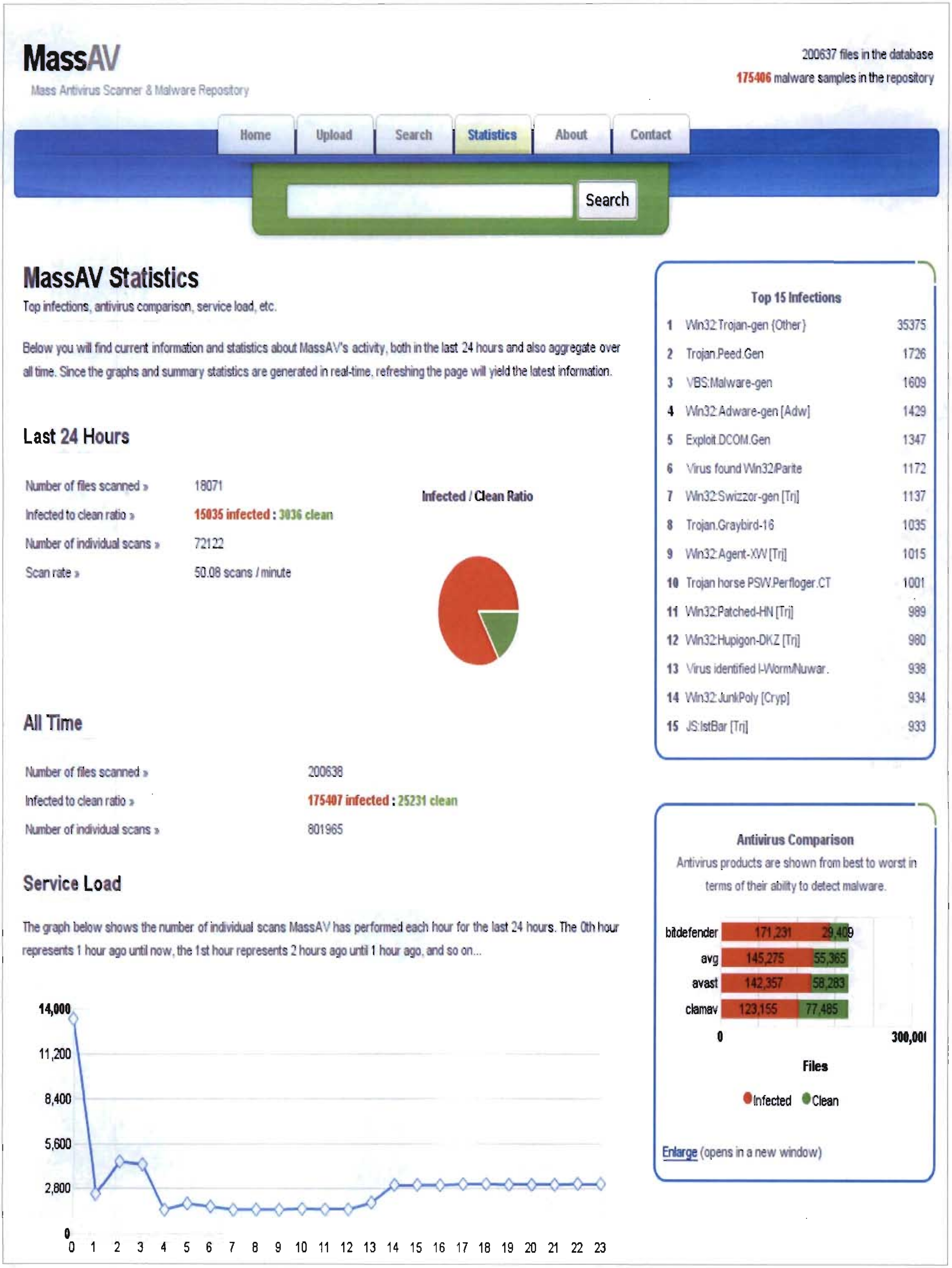
MassAV

Statistical Intrusion Detection and Prevention





Honey Wrappers



200637 files in the database
175406 malware samples in the repository

MassAV Statistics

Top infections, antivirus comparison, service load, etc.

Below you will find current information and statistics about MassAV's activity, both in the last 24 hours and also aggregate over all time. Since the graphs and summary statistics are generated in real-time, refreshing the page will yield the latest information.

Last 24 Hours

Number of files scanned »	18071
Infected to clean ratio »	15035 infected : 3036 clean
Number of individual scans »	72122
Scan rate »	50.08 scans / minute

Infected / Clean Ratio

All Time

Number of files scanned »	200638
Infected to clean ratio »	175407 infected : 25231 clean
Number of individual scans »	801965

Service Load

The graph below shows the number of individual scans MassAV has performed each hour for the last 24 hours. The 0th hour represents 1 hour ago until now, the 1st hour represents 2 hours ago until 1 hour ago, and so on...

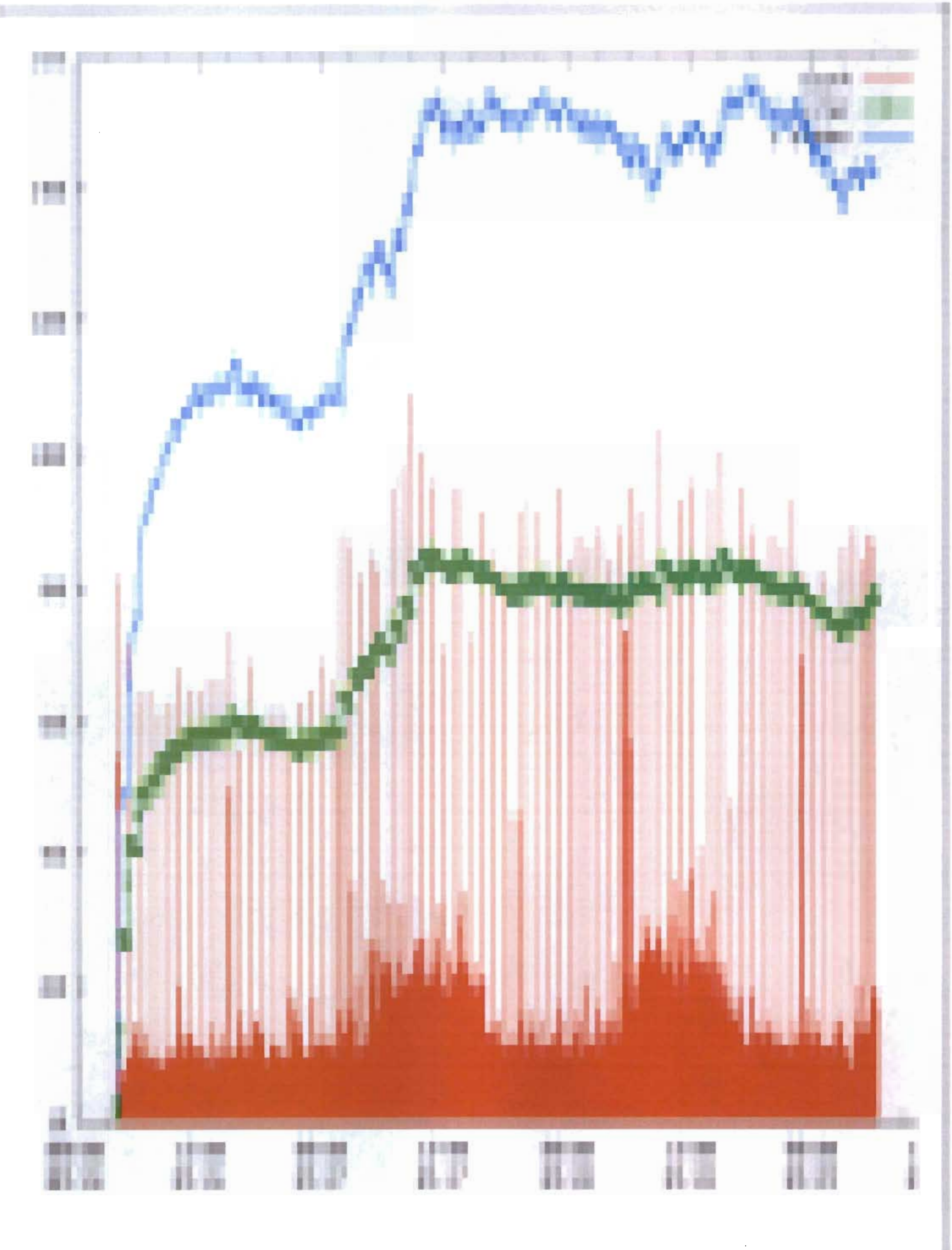
Top 15 Infections

1	Win32:Trojan-gen {Other}	35375
2	Trojan.Peed.Gen	1726
3	VBS:Malware-gen	1609
4	Win32:Adware-gen [Adw]	1429
5	Exploit.DCOM.Gen	1347
6	Virus found Win32/Parite	1172
7	Win32:Swizzor-gen [Trj]	1137
8	Trojan.Graybird-16	1035
9	Win32:Agent-XW [Trj]	1015
10	Trojan horse PSW.Perfloger.CT	1001
11	Win32:Patched-HN [Trj]	989
12	Win32:Hupigon-DKZ [Trj]	980
13	Virus identified I-Worm/Nuwar.	938
14	Win32:JunkPoly [Cryp]	934
15	JS:IstBar [Trj]	933

Antivirus Comparison

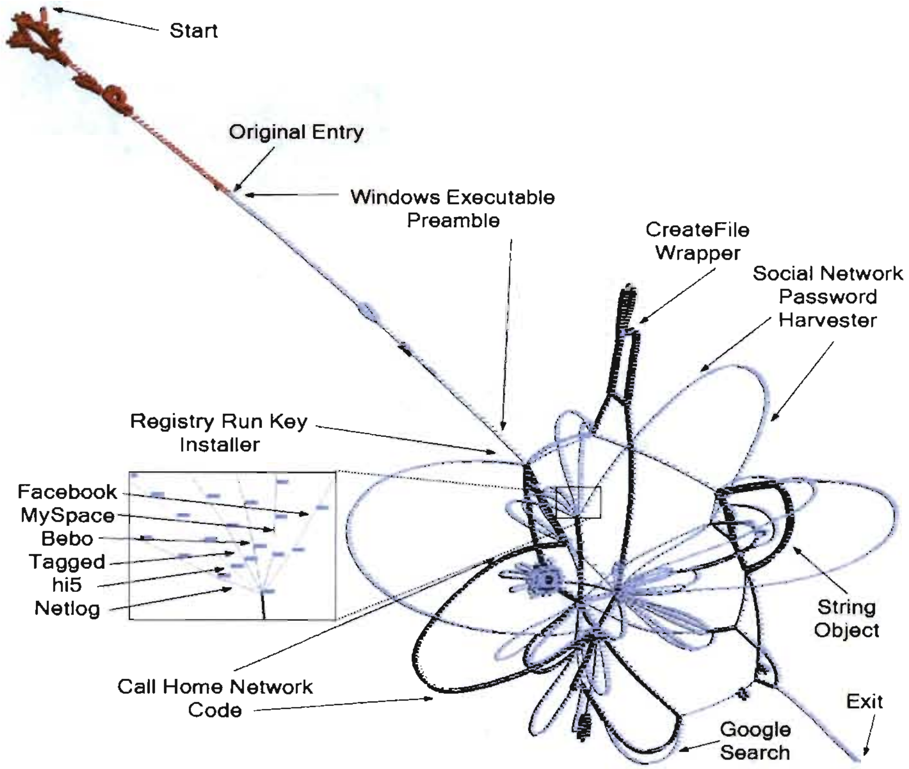
Antivirus products are shown from best to worst in terms of their ability to detect malware.

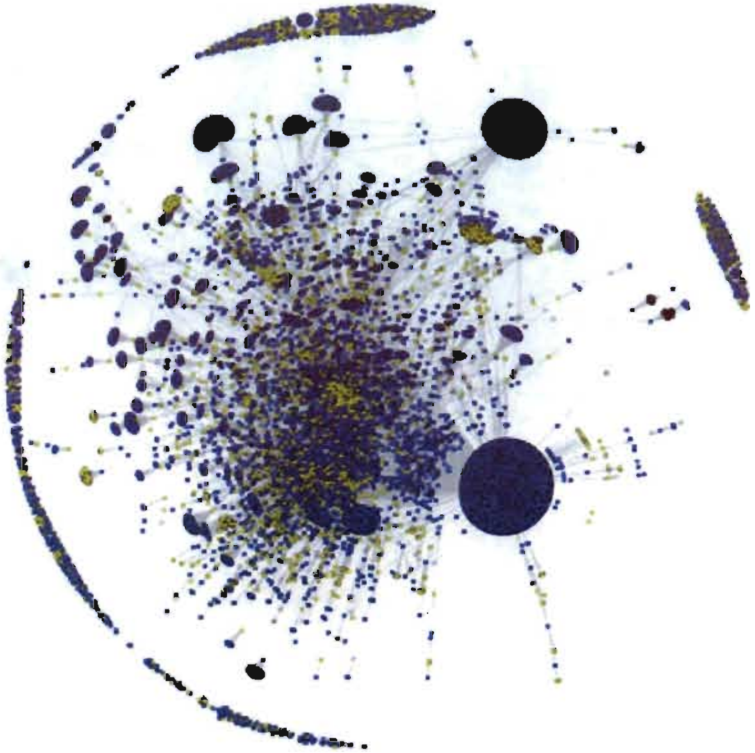
Enlarge (opens in a new window)



Improve Response Capability

Automated Malware Analysis and Classification





Modeling Lateral Movement

Partnerships with Industry

- **Los Alamos National Laboratory welcomes proposals for Cooperative R&D Agreements (CRADAs)**
- **We have existing CRADAs with industry leaders in several verticals**
- **Contact our Technology Transfer Office for details**

Kathleen Herrera McDonald	kathleen_m <at> lanl.gov
David Seigel	seigel <at> lanl.gov