Skip to Main Content
Wiley Online Library
Wiley Online Library
Search
- This Journal
- Anywhere
- Search term Search
  Advanced Search Citation Search
  Search
- Search term Search
  Advanced Search Citation Search
  Search
Login / Register

STATISTICAL ANALYSIS AND DATA MINING

Original Article

Attack chain detection

Joseph Sexton

Corresponding Author

Los Alamos National Laboratory, Los Alamos, NM 87545, USA

Correspondence to: Joseph Sexton (

E-mail address:joesexton0@gmail.com

)
Search for more papers by this author
Curtis Storlie

Los Alamos National Laboratory, Los Alamos, NM 87545, USA

Search for more papers by this author
Joshua Neil

Los Alamos National Laboratory, Los Alamos, NM 87545, USA

Search for more papers by this author
Joseph Sexton

Corresponding Author

Los Alamos National Laboratory, Los Alamos, NM 87545, USA

Correspondence to: Joseph Sexton (

E-mail address:joesexton0@gmail.com

)
Search for more papers by this author
Curtis Storlie

Los Alamos National Laboratory, Los Alamos, NM 87545, USA

Search for more papers by this author
Joshua Neil

Los Alamos National Laboratory, Los Alamos, NM 87545, USA

Search for more papers by this author
First published: 26 September 2015
https://doi.org/10.1002/sam.11296
Cited by: 2
About
Access

PDF

PDF

Tools

- Request permission
- Export citation
- Add to favorites
- Track citation

Share

Give access

Share full text access

Share full text access

Please review our Terms and Conditions of Use and check box below to share full-text version of article.

I have read and accept the Wiley Online Library Terms and Conditions of Use.

Shareable Link

Use the link below to share a full-text version of this article with your friends and colleagues. Learn more.

Copy URL

Share a link

- Email to a friend
- Facebook
- Twitter
- Linkedin
- Google+
- Reddit
- CiteULike

Abstract

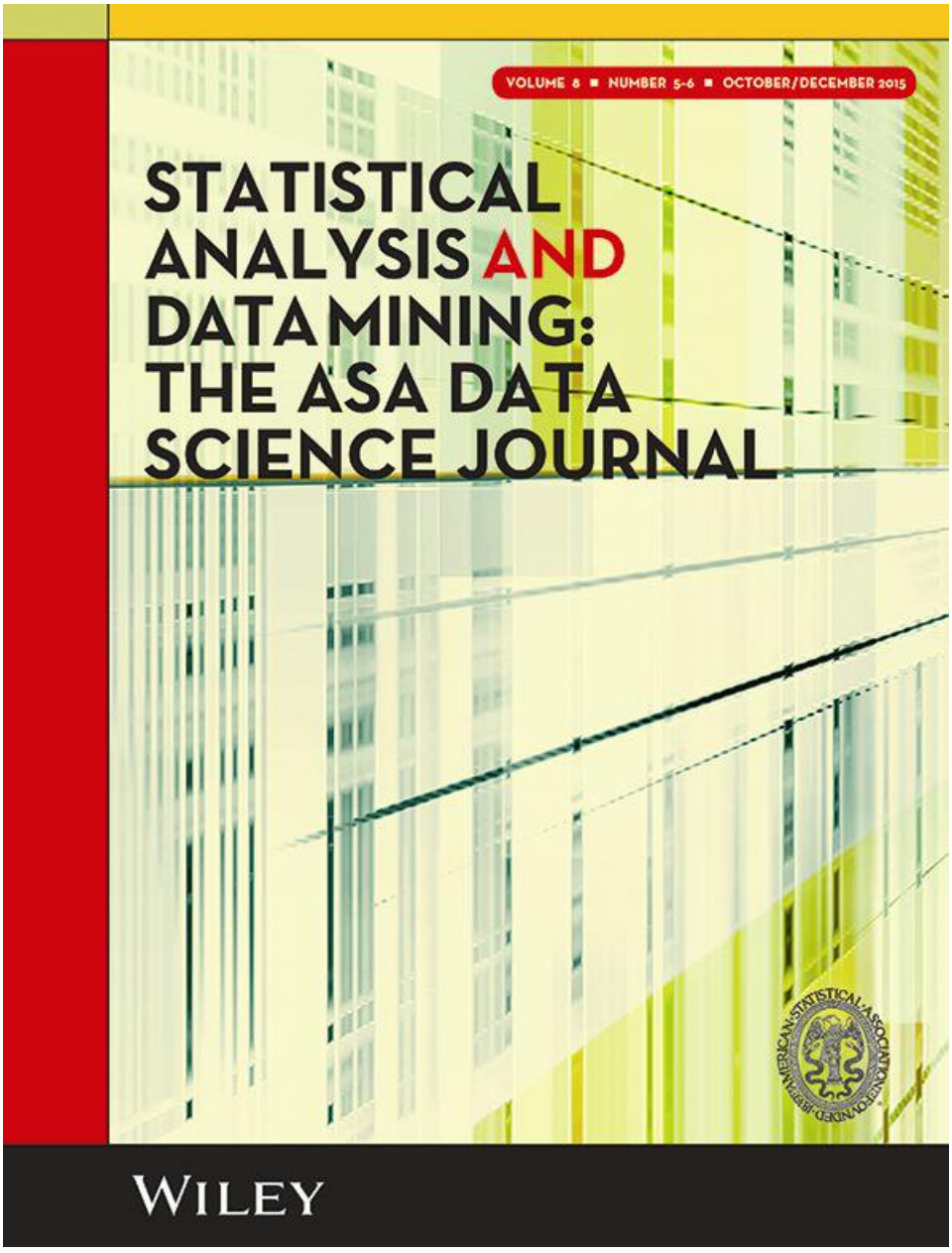
A targeted network intrusion typically evolves through multiple phases, termed the attack chain. When appropriate data are monitored, these phases will generate multiple events across the attack chain on a compromised host. It is shown empirically that events in different parts of the attack chain are largely independent under nonattack conditions. This suggests that a powerful detector can be constructed by combining across events spanning the attack. This article describes the development of such a detector for a larger network. To construct events that span the attack chain, multiple data sources are used, and the detector combines across events observed on the same machine, across local

neighborhoods of machines linked by network communications, as well as across events observed on multiple computers. A probabilistic approach for evaluating the combined events is developed, and empirical investigations support the underlying assumptions. The detection power of the approach is studied by inserting plausible attack scenarios into observed network and host data, and an application to a real-world intrusion is given.

Citing Literature

Number of times cited: 2

2017 IEEE International Conference on Big Data (Big Data) Boston, MA 2017 IEEE International Conference on Big Data (Big Data) IEEE , (2017). 978-1-5386-2715-0 Robert A. Bridges, Jessie D. Jamieson and Joel W. Reed Setting the threshold for high throughput detectors: A mathematical approach for ensembles of dynamic, heterogeneous, probabilistic anomaly detectors , (2017). 1071 1078 8258031 , 10.1109/BigData.2017.8258031 http://ieeexplore.ieee.org/document/8258031/ 2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS) Larnaca, Cyprus 2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS) IEEE , (2016). 978-1-5090-2914-3 Guillaume Brogi and Valerie Viet Triem Tong TerminAPTor: Highlighting Advanced Persistent Threats through Information Flow Tracking , (2016). 1 5 7792480 , 10.1109/NTMS.2016.7792480 http://ieeexplore.ieee.org/document/7792480/



Volume8, Issue5-6

Special Issue: CoDA 2014

October/December 2015

Pages 353-363

- Access
- Related
- Information

- Log in to get access
  INSTITUTIONAL LOGIN >

  Personal login

  Wiley Online Library

  Log in to your account

  Email or Customer ID
  Enter your email
  Password
  Enter your password
  Forgot password?
  Log In
  NEW USER >
  Purchase instant access
  The following formats are available to purchase through ReadCube:

  $6 Rent for 48 hours
  Printing and saving restrictions apply

  $15 Buy cloud access
  Printing and saving restrictions apply

  $38 Buy PDF

  If you previously purchased this article, Sign In to ReadCube.

  CHECKOUT

  Powered by readcube

- Recommend to a librarian

Caption

Additional links

About Wiley Online Library

- Privacy Policy
- Terms of Use
- Cookies
- Accessibility

Help & Support

- Contact Us

Opportunities

- Subscription Agents
- Advertisers & Corporate Partners

Connect with Wiley

- The Wiley Network
- Wiley Press Room

Copyright © 1999-2018 John Wiley & Sons, Inc. All rights reserved

WILEY
Wiley Online Library

Log in to Wiley Online Library

Email or Customer ID
Enter your email
Password
Enter your password
Forgot password?
Log In
NEW USER > INSTITUTIONAL LOGIN >

Wiley Online Library

Change Password

Old Password

New Password

Too Short Weak Medium Strong Very Strong Too Long

Submit

Congrats!

Your password has been changed

Create a new account

Email or Customer ID

Register

Returning user

Wiley Online Library

Forgot your password?

Enter your email address below. If your address has been previously registered, you will receive an email with instructions on how to reset your password. If you don't receive an email, you should register as a new user

Email or Customer ID

Enter your email

RESET PASSWORD

Please check your email for your password reset instructions.

Request Username

Can't sign in? Forgot your username?

Enter your email address below and we will send you your username

Email or Customer ID

Submit

Close

If the address matches an existing account you will receive an email with instructions to retrieve your username