



# SANS Top New Attacks and Threat Report

Date: April 2019 | Author: John Pescatore

In the 2019 SANS Top New Attacks and Threat Report, John Pescatore will provide deeper insight into the threats highlighted during the SANS keynote panel discussion at the 2019 RSA conference. The paper will include practical advice from SANS instructors [Ed Skoudis](#) and [Johannes Ullrich](#) on the critical skills, processes and controls needed to protect their enterprises from these advanced attacks.

## Why Sponsor a Report

### Lead Generation

300-lead guarantee with no cap.

### Branding

Cobrand the whitepaper and webcast with SANS, the global leader in cybersecurity training, certification and research.

### Thought Leadership

Collaborate with our best SANS authors who are at the forefront of the ever-changing war on cyber security.

## About the Author



**John Pescatore** is the SANS Director of Emerging Security Trends and has over 35 years of experience in computer, network and information security. He was Gartner's Lead Security Analyst for 13 years, working with global 5000 corporations and major technology and service providers. John began his career at the National Security Agency, where he designed secure voice systems, and the United States Secret Service, where he developed secure communications and surveillance systems. He has testified before Congress about cybersecurity, was named one of the 15 most-influential people in security in 2008 and is an NSA-certified cryptologic engineer.

## SANS Experts



**Ed Skoudis**  
SANS Fellow  
[@edskoudis](#)



**Johannes Ullrich**  
SANS Fellow  
[@johullrich](#)

## Sponsorship Inclusions

Report	A SANS Analyst will develop a report that includes a deeper insight into the threats highlighted during the panel discussion. Sponsors will receive a final, branded report for their use.
Webcast	The report includes an associated webcast presented by the author. Sponsors will receive the webcast recording for their own promotions. Webcasts are archived for one year after the webcast date. Registrations may still be processed for archive viewing of the webcast. <b>Webcast Date: Coming Soon</b>
Promotion	<b>Report:</b> The 2019 SANS Top New Attacks and Threat Report will be promoted for 5–6 weeks through a weekly email blast to SANS opt-in audience, SANS e-newsletters and social media. <b>Webcast:</b> Promotion of the 2019 SANS Top New Attacks and Threat Report will begin once the webcast has been scheduled. The webcast will be promoted via a weekly email blast to SANS opt-in audience, SANS e-newsletters and social media.
Lead Submission	The initial installment of leads from the webcast will be provided from the downloaded report and webcast within two business days of the live webcast. Additional leads will be provided on a regular basis for the first three months following the webcast. After three months, leads will be provided upon request.

## Additional Sponsorship Opportunities

Associated Single-Sponsored Webcast	Sponsor your own webcast that aligns with the 2019 SANS Top New Attacks and Threat Report. Your webcast will be promoted by SANS. The sponsor will receive a minimum 200-lead guarantee with no cap and continued lead generation as a SANS archive webcast.
Associated Panel Discussion	<b>SANS 2019:</b> Hosted by SANS John Pescatore, the report results will be presented as a Sponsor panel discussion at the SANS 2019 National Event. Attendees will have the opportunity to sit in live and listen to the panel discuss the results of the report.
Associated Paper or Product Review	Publish a custom paper based on a segment of the report that is of interest to you or a product review that calls on the report as an entry point to the review. This associated paper includes a webcast.
Associated Video	Have a SANS expert interview a representative of your company. The sponsor will receive branded video(s) of the interview. The video will also be available on the SANS website. SANS will organize all logistics.

To see examples of other SANS Surveys and Analyst Papers, [click here](#).