SEI Bulletin

Trouble reading this email? View in browser.

Ransomware Research Offers Analysis and Defense Strategies

May 26, 2021 — Earlier this month, a ransomware attack crippled the flow of fuel to the east coast. Colonial Pipeline joined an ever-growing list of victims, including hospitals, schools, and entire municipalities, whose digital assets have been encrypted and held for ransom by criminals.

Cybersecurity experts in the SEI's CERT Division have been studying how ransomware works and how to defend against it. Check out the blog posts, podcasts, and papers below for the latest SEI research on this increasingly common and costly cyber attack.

Selected CERT Ransomware Resources

3 Ransomware Defense Strategies - Blog Post
Marisa Midler explores strategies to mitigate two main ransomware attack vectors, RDP attacks and software vulnerabilities, as well as how to protect against data exfiltration.

Three Places to Start in Defending Against Ransomware - Blog Post
Tim Shimeall covers three initial efforts that will make ransomware attacks more

difficult for attackers and less costly to organizations.

Ransomware as a Service (RaaS) Threats - Blog Post
Marisa Midler explores the economics behind why ransomware remains a top tool for cybercrime and presents the current active ransomware variants that utilize ransomware as a service (RaaS).

Ransomware: Best Practices for Prevention and Response - Blog Post
Alexander Volynkin, Jose Morales, and Angela Horneman spell out several best practices for prevention and response to a ransomware attack.

Ransomware: Evolution, Rise, and Response - Podcast
Marisa Midler and Tim Shimeall discuss steps and strategies that organizations can adopt to minimize their exposure to the risks and threats associated with ransomware.

Current Ransomware Threats - White Paper
Marisa Midler, Kyle O'Meara, and Alexandra Parisi discuss ransomware, including an explanation of its design, distribution, execution, and business model.

An Updated Framework of Defenses Against Ransomware - White Paper
Timur Snoke and Tim Shimeall frame an approach for defending against ransomware-as-a-service (RaaS) as well as direct ransomware attacks.

SEI News

Nominations Sought for 2021 Northrop Software Architecture Award
Nominate an individual or team by June 15 for success through architecture, leadership, persistent change, and a new perspective.

Registration Open for Software Engineering Workshop for Educators 2021
The SEI invites college-level educators of all areas of software engineering to join the 18th annual workshop virtually.

DevSecOps Days Pittsburgh 2021 Opens Registration
The free meeting of DevSecOps practitioners will be held virtually on June 16.

See more news »

Latest Blogs

Taking DevSecOps to the Next Level with Value Stream Mapping
Nanette Brown explores the relationship between DevSecOps and value stream mapping, both of which are rooted in the Lean approach to systems and workflow.

Software Engineering for Machine Learning: Characterizing and Detecting Mismatch in Machine-Learning Systems
Grace Lewis and Ipek Ozkaya describe the SEI's creation and assessment of empirically validated practices to guide the development of machine-learning-enabled systems.

Integrating Safety and Security Engineering for Mission-Critical Systems
Sam Procter and Sholom Cohen describe how SEI research on safety and security engineering is applied to improve coordination of the safety and security communities.

See more blogs »

Latest Podcasts

Moving from DevOps to DevSecOps
Hasan Yasar discusses how organizations can transition from DevOps to DevSecOps.

My Story in Computing with Dave Zubrow
David Zubrow discusses his career, from an applied history and social sciences PhD to a manager and technical leader at the SEI.

Mission-Based Prioritization: A New Method for Prioritizing Agile Backlogs
Keith Korzec discusses the Misson-Based Prioritization method for prioritizing Agile backlogs.

See more podcasts »

Latest Publications

Foundation of Cyber Ranges
This report details the design considerations and execution plan for building high-fidelity, realistic virtual cyber ranges that deliver maximum training and exercise value for cyberwarfare participants.

Using Value Engineering to Propel Cyber-Physical Systems Acquisition
This paper investigates the adaptation of value engineering (VE) methods into the acquisition of software-intensive weapon systems.

Prioritizing Vulnerability Response: A Stakeholder-Specific Vulnerability Categorization (Version 2.0)
Version 2.0 of a Stakeholder-Specific Vulnerability Categorization (SSVC) is formed of decision trees and avoids some problems with the Common Vulnerability Scoring System (CVSS).

See more publications »

Latest Videos

Webcast - Software Supply Chain Concerns for DevSecOps Programs
Aaron Reffett and Richard Laughlin explore the important architectural aspects of DevSecOps that are impacted by the software supply chain.

Webcast - How Do We Teach Cybersecurity?
Rotem Guttman shares the lessons he's learned over a decade of developing engaging, immersive training and evaluation environments.

Webcast - How I Learned to Stop Worrying and Love SLAs
Matt Butkovic and Alan Levin discuss how cybersecurity SLAs are vital to the success of third-party relationships and a core component of sound governance.

Upcoming Events

DevSecOps Days Pittsburgh 2021, June 16
Join leading DevSecOps professionals who are changing the world of software engineering.

Software Engineering Workshop for Educators, August 3-5
The annual Workshop for Educators to foster an ongoing exchange of ideas among educators whose curricula include the subjects of software architecture and software product lines.

AI World Government 2021, October 18-19
SEI experts will participate in this two-day forum to educate federal agency leaders on proven strategies and tactics to deploy AI and cognitive technologies.

Note: The SEI is evaluating all upcoming courses, conferences, and events case-by-case in light of COVID-19 developments. Check individual event pages for the latest information.

See more events »

Upcoming Training

Insider Threat Vulnerability Assessor Training
June 8-10, 2021 (SEI, Live Online)

Insider Threat Program Manager: Implementation and Operation
July 20-22, 2021 (SEI, Live Online)

Insider Threat Analyst
August 10-12, 2021 (SEI, Live Online)

Note: The SEI is evaluating all upcoming courses, conferences, and events case-by-case in light of COVID-19 developments. Check individual training pages for the latest information. You may also contact us at courseregistration@sei.cmu.edu or +1-412-268-7388.

See more courses, including live-online and eLearning offerings »

Employment Opportunities

Senior Cybersecurity Operations Researcher

Senior Risk Engineer

All current opportunities »

Carnegie Mellon University
Software Engineering Institute