



RoT: Ransomware of Things

- › How ransomware is evolving and could potentially take over every single device?
- › Jackware + IoT
- › How ransomware family evolved and what to expect



AUTHOR

Stephen Cobb
ESET Senior Security
Researcher

[Internet of Things](#) [PDF] from DHS (US Department of Homeland Security), and [NIST Special Publication 800-160](#) [PDF]. The full title of the latter is *Systems Security Engineering Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*. NIST is the National Institute of Standards and Technology, part of the US Department of Commerce, and over the years the agency has exerted a positive influence on many aspects of cybersecurity. Hopefully, these efforts, and the many others around the world, will help us make progress in 2017 towards securing our digital lives against those who choose to abuse technology to extort us.

Finally, evidence that we might be making some progress, at least in terms of public awareness of the potential for the IoT to bring problems as well as perks and productivity gains, comes from a different kind of publication, the results of an ESET consumer survey. Reported under the title of "[Our Increasingly Connected Digital Lives](#)" the survey revealed that more than 40 percent of American adults were not confident that IoT devices are safe and secure. Furthermore, more than half of respondents indicated that privacy and security concerns had discouraged them from purchasing an IoT device. Could the combination of consumer sentiment and government guidance lead companies to make the IoT more resistant to abuse? We may find out in 2017.

