RoT: Ransomware of Things

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

AUTHOR

Stephen Cobb
ESET Senior Security Researcher

1

RoT: Ransomware of Things

One of the trends that I found most worrying in 2016 was the willingness of some humans to participate in the following three activities at scale: hold computer systems and data files hostage (ransomware); deny access to data and systems (Distributed Denial of Service or DDoS); infect some of the things that make up the Internet of Things (IoT). Sadly, I think these trends will continue in 2017 and there is potential for cross-pollination as they evolve. For example, using infected IoT devices to extort commercial websites by threatening a DDoS attack, or locking IoT devices in order to charge a ransom, something I like to call jackware.

Past and future threats

Abusing information systems to extort money is almost as old as computing itself. Back in 1985, an IT employee at a US insurance company programmed a logic bomb to erase vital records if he was ever fired; two years later he was, and it did, leading to the first conviction for this type of computer crime. Malware that used encryption to hold files for ransom was seen in 1989, as David Harley recounts. By 2011, locking computers for a ransom was "stooping to new lows" as my colleague Cameron Camp put it.

So how might these elements evolve or merge in 2017? Some people have been referring to 2016 as "The Year of Ransomware" but I'm concerned that a future headline will read: "The Year of Jackware." Think of jackware as malicious software that seeks to take control of a device, the primary purpose of which is not data processing or digital communications. A good example is a "connected car" as many of today's latest models are described. These cars perform a lot of data processing and communicating, but their primary purpose is to get you from A to B. So think of jackware as a specialized form of ransomware. With regular ransomware, such as Locky and Cryptolocker, the malicious code encrypts docu-ments on your computer and demands a ransom to unlock them. The goal of jack-ware is to lock up a car or other device until you pay up.

A victim's eye view of jackware might look like this: on a cold and frosty morning I use the car app on my phone to remote start my car from the comfort of the kitchen, but the car does not start. Instead I get a text on my phone telling me I need to hand over X amount of digital currency to re-enable my vehicle. Fortunately, and I stress this: jackware is, as far as I know, still theoretical. It is not yet "in the wild".

Unfortunately, based on past form, I don't have great faith in the world's ability to stop jackware being developed and deployed. We have already seen that a car company can ship more than a million vehicles containing vulnerabilities that could have been abused for jackware: the Fiat Chrysler Jeep problem that was all over the news in 2015. Just as serious as those vulnerabilities was FCA's apparent lack of planning for vulnerability patching in the vehicle design process. It is one thing to ship a digital product in which 'holes' are later discovered – in fact, this is pretty

much inevitable – but it is a different and more dangerous thing to ship digital products without a quick and secure means of patching those holes.

While most "car hacking" research and discussion centers on technical issues within the vehicle, it is important to realize that a lot of IoT technology relies on a support system that extends well beyond the device itself. We saw this in 2015 with VTech, a player in the IoCT space (as in Internet of Children's Things). Weak security on the company's website exposed personal data about children, reminding everyone just how many attack surfaces the IoT creates. We also saw this infrastructure issue in 2016 when some Fitbit accounts had problems (to be clear, the Fitbit devices themselves were not hacked, and Fitbit seems to take privacy seriously). Also this year, bugs were discovered in the online web app BMW ConnectedDrive, which connects BMWs to the IoT. For example, you can use it to regulate your home's heating, lights, and alarm system from inside your vehicle. The possibility that the features and settings of an in-vehicle system could be remotely administered through a portal that could be hacked is unsettling to say the least. And reports of vehicular cyber-insecurity keep coming, like this Wi-Fi enabled Mitsubishi, and hacked radios used to steal BMWs, Audis, and Toyotas.

While I originally thought of jackware as an evolution of malicious code targeting vehicles, it became clear that this trend could manifest itself more broadly: the Ransomware of Things (RoT). A chilling story from Finland shows one direction that this might take (DDoS attack halts heating in Finland during winter). While there was no indication of ransom demands in the reports, you can imagine this as the next step. Want us to stop DDoSing the heating system? Pay up!

Stopping the RoT

To stop the IoT from becoming home to the RoT, several things need to happen. First is the technical sphere, where the challenge of implementing security on a vehicular platform is considerable. Traditional security techniques, like filtering, encrypting, and authenticating, can consume costly processing power and bandwidth, adding overhead to systems, some of which need to operate with very low latency. Security techniques like air-gapping and redundancy could add significantly to the cost of vehicles. And we know controlling costs has always been critical to car manufacturers, down to the last dollar.

The second sphere where action is required is policy and politics. The outlook here is not good: There has been a collective international failure to prevent a thriving criminal infrastructure evolving in cyberspace, one that now threatens every innovation in digital technology you can think of, from telemedicine to drones to big data to self-driving cars. For example, as alluded to in ESET's *Trends 2017* chapter **"Challenges and implications of Cybersecurity Legislation,"** concerned politicians failed to pass legislation in 2016 that would help secure the smart grid, despite bipartisan support.

To be clear, terms like RoT and jackware are not intended to cause alarm. They symbolize things that could come to pass if we do not do enough in 2017 to prevent them from becoming a reality. So let me end with some positive developments. First, a variety of government agencies are stepping up their efforts to make the IoT more secure. In 2016 we saw publication of the Strategic Principles for Securing the

Terms like RoT and jackware are not intended to cause alarm. They symbolize things that could come to pass if we do not do enough in 2017 to prevent them from becoming a reality.

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.

About ESET

Since 1987, ESET® has been developing award-winning security software that now helps over 100 million users to Enjoy Safer Technology. Its broad security product portfolio covers all popular platforms and provides businesses and consumers around the world with the perfect balance of performance and proactive protection.

The company has a global sales network covering more than 200 countries and territories, and regional offices in Bratislava, San Diego, Singapore and Buenos Aires. For more information visit www.eset.com or follow us on LinkedIn, Facebook and Twitter.

www.eset.com

ENJOY SAFER TECHNOLOGY™