



CRIME, TERROR AND THE INTERNET OF THINGS

A WIKISTRAT CROWDSOURCED SIMULATION

November 2016



TABLE OF CONTENTS

1

INTRODUCTION

2

METHODOLOGY

4

DEEP SURVEILLANCE USING SMART HOME PLATFORMS

IoT appliances in smart homes could be used to spy on individuals

5

SEX CRIMES RELYING ON THE IOT

An attacker could know exactly when and where to strike

6

DAMAGING CORPORATE REPUTATION

The most damaging cyberattacks may be conducted by competing firms

7

INSIDER INFORMATION

The wealthy could find themselves under surveillance by criminals who break into their IoT devices

8

ATTACKS ON SMART CITIES

The potential damage resulting from a cyberattack on a smart city is huge

9

TAKEAWAYS



INTRODUCTION

The Internet of Things (IoT) is rapidly growing in breadth and use – the number of web-connected devices is projected to grow significantly over the next ten years. The economic impact of the IoT [could reach \\$11.1 trillion per year by 2025](#).

There will inevitably be a dark side to this development. Criminals and terrorists are traditionally adept at using emerging and disruptive technologies to their advantage. Among recent examples: A 14-year-old hacker took control of a tram system in Poland and caused two trains to collide in 2008. A hacktivist broke into water utilities in Texas in 2011. In 2015, various hackers broke into wireless baby monitors and webcams and remotely spied on – and even communicated to – infants.

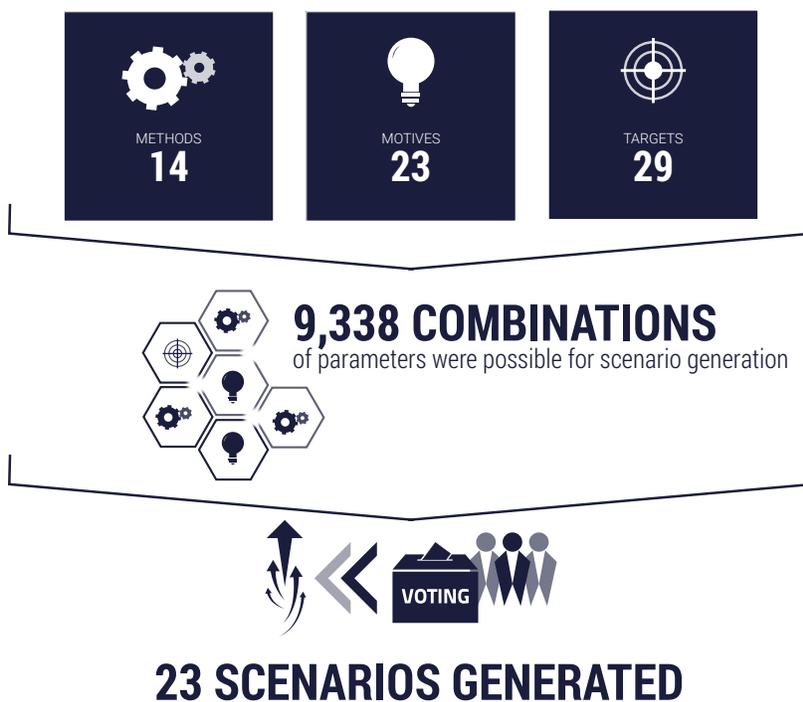
The frequency and severity of such incidents can be [expected to rise](#). The number of security breaches whose origin can be tracked to cloud-based devices rose by 152 percent between 2014 and 2015. The FBI has urged Americans to be vigilant with IoT devices. As such, it is imperative to consider scenarios for future crimes and terrorist attacks that could involve the IoT.

During a simulation entitled “Crime, Terror and the Internet of Things” (which ran from June 20 to 27), 47 Wikistrat analysts generated and appraised dozens of potential targets, methods and motives for acts of crime and terror related to the IoT, and developed a large number of scenarios that could be of service to anyone involved in the field of security.

METHODOLOGY

Wikistrat used a crowdsourced version of *general morphological analysis* in this five-phase project. Potential scenarios were considered to be made up of three components (referred to as parameters): *methods*, *targets* and *motives*. After generating entries for each parameter, analysts ranked each according to the potential resultant impact (in the case of targets or motives) or likelihood of use (in the case of methods).

A morphological field was then created based on the 9,338 scenarios generated via each possible combination of three scenario components (one from each parameter). Combinations of high interest were identified via an algorithm which utilized parameter voting results; analysts chose 23 such combinations as a basis for scenario development. Lastly, analysts discussed, developed and then ranked these scenarios according to their relative plausibility.



This report contains the five scenarios that were deemed the most plausible by Wikistrat's analysts.



DEEP SURVEILLANCE USING SMART HOME PLATFORMS

Smart homes are rapidly turning from an abstract concept into a reality. IoT devices can be found everywhere – e.g., smart door locks, virtual assistants like Amazon Echo, smart baby monitors, smart thermostats and even smart grills. All of these can connect to the Internet and communicate with their owners via dedicated apps or platforms.

However, such platforms can be hacked – as was demonstrated in 2016, when inherent flaws in Samsung’s Smart Home platform allowed hackers to control home lighting and even door locks with ease. By the time the flaw was discovered, the system had already been installed in tens of thousands of homes.

Wikistrat’s analysts suggest that IoT appliances in smart homes could be used to spy on individuals for the purposes of blackmail. Such crimes seem highly likely in light of contemporary use of ransomware – especially should hackers tap into webcams. People may even find themselves locked outside their own homes, forced to pay a few bitcoins in ransom via their smartphones to regain entry.

Wikistrat’s analysts suggest that IoT appliances in smart homes could be used to spy on individuals for the purposes of blackmail. Such crimes seem highly likely in light of contemporary use of ransomware – especially should hackers tap into webcams.



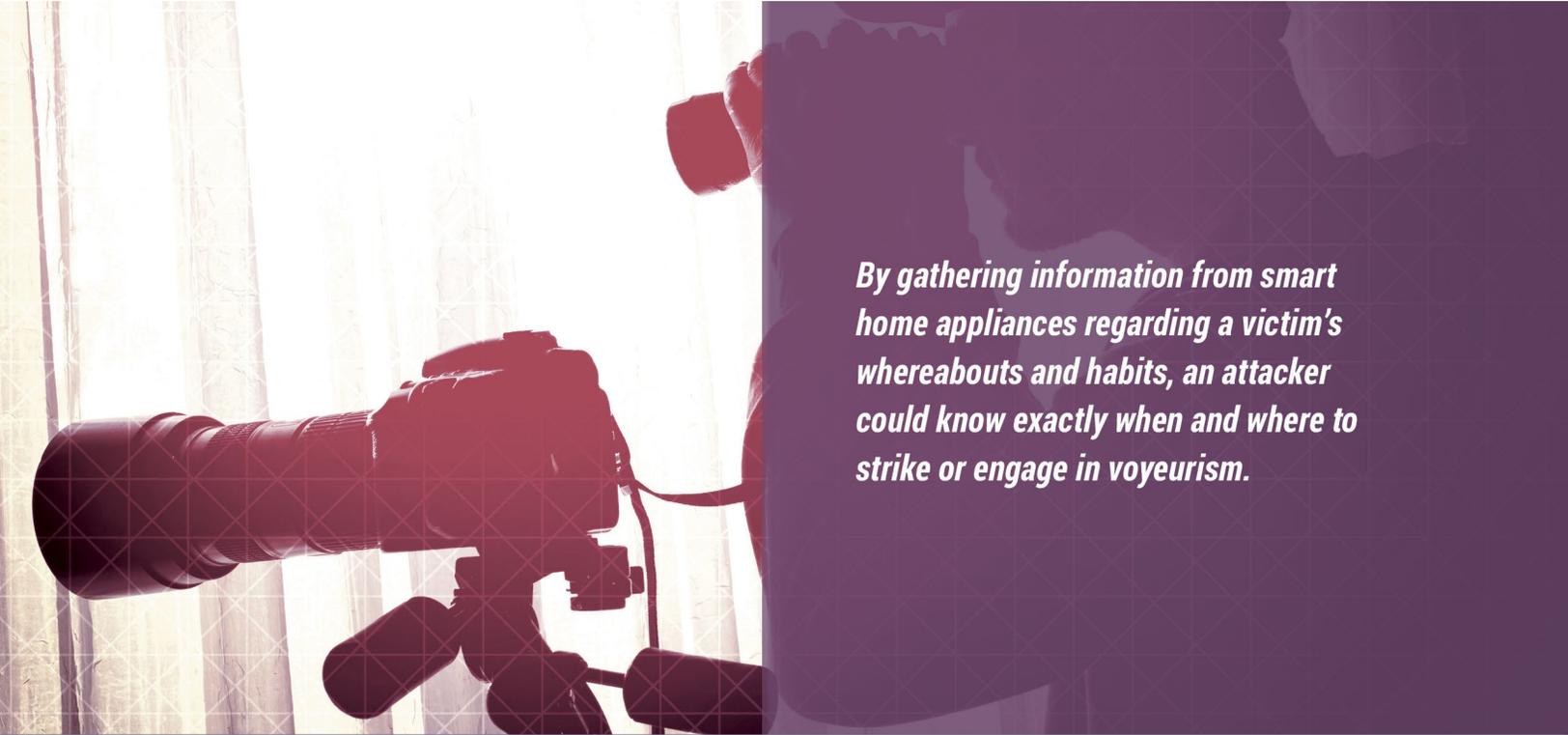


SEX CRIMES RELYING ON THE IoT

Sex crimes could be committed via malicious use of the IoT – including sexual assault. By gathering information from smart home appliances regarding a victim's whereabouts and habits, an attacker could know exactly when and where to strike or engage in voyeurism.

One of the most plausible scenarios highlighted by the analysts was theft of amateur sex videos. Such videos may have been recorded intentionally by victims or via hacker control of home cameras and microphones. These videos could be used for blackmail or even for political gain in cases where politicians are recorded.

Such crimes have already been committed. Miss Teen USA 2013 Cassidy Wolf was the victim of a "sextortion" scheme involving hacked webcams and explicit photos being illegally accessed. A subsequent global investigation into the hacking of webcams led to 97 arrests in 2014.



By gathering information from smart home appliances regarding a victim's whereabouts and habits, an attacker could know exactly when and where to strike or engage in voyeurism.



DAMAGING CORPORATE REPUTATION

While there is a distinct impression among laypeople that only hackers and hardened criminals are involved in cybercrimes, corporations also use cybercrime to fight and gain information about each other. Many companies would dearly wish to anonymously demonstrate how easily their opponents' security can be breached in order to tarnish their reputation and thus gain relative public favor.

Wikistrat's analysts believe it is especially plausible that connected appliances in hospitals and health facilities will be hacked in order to undermine the public's trust therein. Indeed, any corporation that relies on the IoT or web-connected devices – including on their factory floors – must recognize that such devices are vulnerable to attack from competitors' own cyber divisions or hired hackers.

This means that the most damaging cyberattacks of the future may not be conducted by criminals or terrorists, but instead by private firms in competition with one another. Companies that only prepare to defend against the former could leave themselves vulnerable to an attack from the latter.



The most damaging cyberattacks of the future may not be conducted by criminals or terrorists, but instead by private firms in competition with one another.



INSIDER INFORMATION

Sophisticated technologies, such as wearable devices and smart home appliances and platforms, are often first used by the wealthy. As a result – particularly at the early stages when these technologies are not as secure as they should be – the wealthy could find themselves under surveillance by criminals who break into their IoT devices and thereby track their every move.

One purpose of this surveillance would be to understand these people’s financial decisions and to act accordingly in advance. Criminals and criminal organizations that manage to conduct such attacks could remain unknown and unseen for a long time while becoming consistently richer by means of their insider information.

This scenario is particularly relevant to “C-level” executives and board members of private firms. They may find themselves under constant surveillance by rival companies or criminals. Their meetings and discussions may be monitored. Due to the emerging nature of both the threat and the equipment being used at such meetings, it is quite possible that this danger will be left unaddressed.



The wealthy could find themselves under surveillance by criminals who break into their IoT devices and thereby track their every move.



ATTACKS ON SMART CITIES

The potential damage resulting from a cyberattack on a smart city is huge. Cyberworms could self-propagate through the millions of connected devices in a city and retrieve valuable and private information. Such viruses could even take control over some of these devices, which could then be used to launch distributed denial of service (DDoS) attacks or even hold a city hostage.

Analysts highlighted two very plausible scenarios relating to cyberattacks on smart cities:



CYBERATTACK AS A PRECURSOR TO A PHYSICAL ATTACK

A capable terrorist group remotely conducts a cyberattack to essentially shut down or disrupt the ongoing affairs of a city. The cyberattack would then enable and be followed by a more conventional attack by terrorists with guns or explosives.



HACKTIVISTS DISRUPT CITY FUNCTIONS

Cyberattackers shut down or disrupt key infrastructure sites in a smart city, leading to political embarrassment, economic damage and potentially even loss of life. Such incidents are especially likely during high-profile political, sporting or economic events.

Manufacturers of web-connected infrastructure – e.g., street cameras, lights, sewage systems – need to anticipate that their devices will become a tempting target for attackers. Those devices may not only be targeted to impede their usual functioning, but because attackers wish to add them to a malicious botnet.¹ This may even leave the manufacturers open to claims of negligence in case a crime is enacted by botnets which involve their devices.

¹ A botnet is an unwitting network of web-connected, malware-infected computers used for criminal purposes

TAKEAWAYS

The Internet of Things has great potential to improve the functions of many systems in the coming decade. But as former law enforcement officer and author Marc Goodman has said, “When everything is connected, everyone is vulnerable.” The virtual world is riddled with hackers, worms, viruses and hacktivists, and it is a safe bet that the IoT – as the bridge between the virtual and the physical world – will enable these actors to move into the physical world as well.

Wikistrat has analyzed the most important IoT targets, the most likely methods attackers will use and the motives behind such attacks. Our research suggests that public infrastructure is most at risk in terms of security, as are private citizens in their homes. These two very different targets reveal some of the inherent difficulties that lawmakers and security experts must deal with regarding the IoT – as each requires a very different strategy for successful cyberdefense.

- » **Defenders:** While private citizens are ordinarily protected by large industries which provide them with services, public infrastructure is generally protected by the government or relatively small subcontractors.
- » **Failure Allowance:** While security measures enacted for private citizens can be allowed to fail in a small fraction of cases, any failure of public infrastructure will have dire consequences.
- » **Sophistication of Attackers:** Hackers who attack IoT appliances in the hands of private citizens will not require a high level of sophistication to cause harm, in part due to the largely standardized build of such appliances. On the other hand, hackers who wish to cause real harm to public infrastructure will need to collaborate with experts therein – water system engineers, traffic engineers and so forth.

ABOUT US



2500+
ANALYSTS



CUTTING-EDGE INTELLIGENCE SERVICES



Crowdsourced
Simulations



Wargames



Red-Teaming



Intelligence
Monitoring

Wikistrat is the world's first crowdsourced consultancy. It leverages a global network of subject-matter experts via a patent-pending "Collaborative Competition" methodology to provide a variety of analytic services. Scenario generation, policy planning, risk assessment and red-teaming exercises are conducted by Wikistrat on a real-time, interactive online platform.

WHAT MAKES WIKISTRAT UNIQUE



Geographically
dispersed
analysts



Competition
between
ideas



Collaboration
in real time



Fully
transparent

VALUE TO CLIENTS



Fuller, fresher
insights



Rapid



Cost-effective

ABOUT THE AUTHOR



DR. ROEY TZEZANA

Senior Analyst

Dr. Roey Tzezana holds a PhD in Nanotechnology from the Technion – Israel Institute of Technology and is a Research Fellow at the Blavatnik Interdisciplinary Cyber Research Center (ICRC) at Tel Aviv University. He is the author of *Guide to the Future*. The author wishes to thank ICRC for their support of the research.

DISCLAIMER

This report is for informational purposes only and does not constitute financial, investment, economic, financial planning, trading or any other advice. You should consult with a competent independent financial advisor before making any investment or other decisions and should independently verify information on which you rely. The report is provided without any express or implied warranty of any kind including warranties of accuracy, completeness, or fitness for any particular purpose. Without limitation, although we have prepared this report based on sources we believe to be reliable, legally derived, and unbiased, we can provide no assurance with respect to the objectivity or any other aspect of its content. In addition and without limitation, this report may contain predictions, estimates or other information that might be considered forward-looking or predictive. Such statements are subject to risks and uncertainties that could cause actual results to differ materially. We assume no obligation to update the report or any part thereof or to correct any inaccurate or outdated information and reserve the right to remove or modify the report, in each case without notice to you or any other party. Without limitation, this report is subject to the Terms of Service posted on our internet website at www.wikistrat.com.

CRIME, TERROR AND THE INTERNET OF THINGS

AUTHOR:

Dr. Roey Tzezana

EDITOR:

Steve Keller

GRAPHIC DESIGNER:

Sheila Elizan

For more information on Wikistrat's crowdsourced solutions and systems, contact: info@wikistrat.com

www.wikistrat.com

