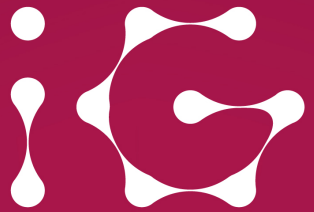


INNOLYTICS
GROUP

Cybersecurity

Cyber Attack Background

INNOLYTICS GROUP

6.4 billion
The number of fake emails sent worldwide – every day[1]

1,464
The number of government officials in one state using "Password123" as their password[2]

50%
The number of local authorities in England relying on unsupported server software[3]

2 million
The number of stolen identities used to make fake comments during a US inquiry into net neutrality[4]

1,946,181,599
The total number of records containing personal and other sensitive data compromised between January 2017 and March 2018[5]

US$729,000
The amount lost by a businessman in a scam combining "catphishing" and "whaling"[6]

550 million
The number of phishing emails sent out by a single campaign during the first quarter of 2018[7]

US$3.62m
The average cost of a data breach last year[8]

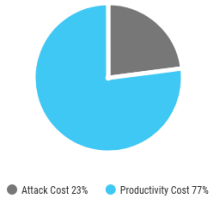
Almost half of all companies have over 1,000 sensitive pieces of information that are not protected

Attacks on healthcare are expected to increase by

400%

in 2020

The biggest cost from a cyber attack is productivity



The cost of cyber crime is expected to exceed

$6 Trillion

Annually by 2021

- **88 records** were lost or stolen **every second** in 2017
- Cybersecurity Ventures predicts that a **business** will fall victim to a ransomware attack every **11 seconds** by **2021**.


TOWER 2
Franciscan A, B, C & D • Imperial Ballroom A & B
Continental Ballroom 1-9
BALLROOM
abundance 360

META-TRENDS (Part-1):

1. Increasing global abundance.

2. Accelerating Demonetization & Democratization

3. *Everyone*, everywhere is connected at gigabit speeds.

4. *Everything* , everywhere is connected (IoT/IoE).

5. You can know anything, anytime, anywhere.

It's not just people being connected, we are connecting everything, everywhere…

2020: 20B+ connected devices & >1 Trillion Sensors

2030: 500B+ connected devices & >100 Trillion Sensors

IoT TO CREATE $6.2 TRILLION OF NEW ECONOMIC VALUE BY 2025 - *McKinsey*

Cyber Attack Surface – What's Next?

INNOLYTICS GROUP

- **Half a billion wearable devices** will be **sold worldwide in 2021**, up from roughly 310 million in 2017.
- The world will need to cyber protect **300 billion passwords** globally by **2020**.
- There are **more than 111 billion lines of new software code** being produced each year — which introduces a massive number of vulnerabilities that can be exploited.
- There will be **100 trillion networked sensors in 10 years from now**.
- More than **20 million connected cars** will ship with built-in software-based security technology by **2020**
- Spanish telecom provider Telefonica states **by 2020**, **90 percent of cars** will be **online**, compared with just 2 percent in 2012

Dark Consequences of “Internet of Everything”

INNOLYTICS GROUP

1. **“Attack surface”** of private and corporate users grows.
2. More data and connected devices online – **more possibilities for attacks** and **devastation** (example: factory online).
3. Vulnerability of **IoT devices** – simple, cheap, easy to hack, massive number.
4. Growing **disproportion of attacks’ cost/damage** (Saudi Aramco and drones).
5. New **Threats** – for example to **Reputation**.

What about users?

INNOLYTICS GROUP

Languages

Français

Edit links

Top 25 most common passwords by year according to SplashData

Rank	2011[4]	2012[5]	2013[6]	2014[7]	2015[8]	2016[3]	2017[9]	2018[10]
1	password	password	123456	123456	123456	123456	123456	123456
2	123456	123456	password	password	password	password	password	password
3	12345678	12345678	12345678	12345	12345678	12345	12345678	123456789
4	qwerty	abc123	qwerty	12345678	qwerty	12345678	qwerty	12345678
5	abc123	qwerty	abc123	qwerty	12345	football	12345	12345
6	monkey	monkey	123456789	123456789	123456789	qwerty	123456789	111111
7	1234567	letmein	111111	1234	football	1234567890	letmein	1234567
8	letmein	dragon	1234567	baseball	1234	1234567	1234567	sunshine
9	trustno1	111111	iloveyou	dragon	1234567	princess	football	qwerty
10	dragon	baseball	adobe123[a]	football	baseball	1234	iloveyou	iloveyou
11	baseball	iloveyou	123123	1234567	welcome	login	admin	princess
12	111111	trustno1	admin	monkey	1234567890	welcome	welcome	admin
13	iloveyou	1234567	1234567890	letmein	abc123	solo	monkey	welcome
14	master	sunshine	letmein	abc123	111111	abc123	login	666666
15	sunshine	master	photoshop[a]	111111	1qaz2wsx	admin	abc123	abc123
16	ashley	123123	1234	mustang	dragon	121212	starwars	football
17	bailey	welcome	monkey	access	master	flower	123123	123123

Case Study: Fish Tank Thermometer

INNOLYTICS GROUP

BUSINESS INSIDER DEUTSCHLAND INTERNATIONAL

Hackers once stole a casino's high-roller database through a thermometer in the lobby fish tank

BI Oscar Williams-Grut, Business Insider
15.04.2018, 09:08

FACEBOOK LINKEDIN TWITTER EMAIL PRINT

An aquarium at a casino – but not the one in question. Ethan Miller/Getty Images

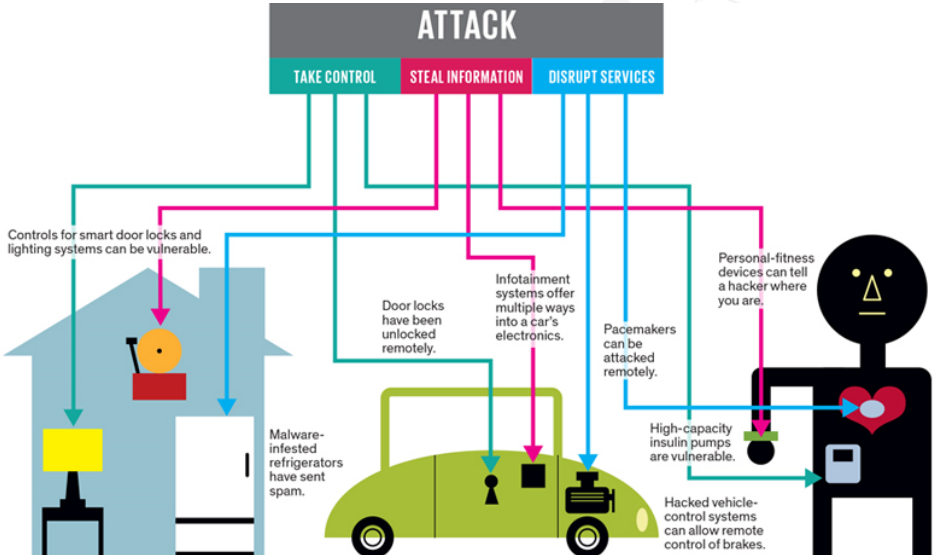
"The chain is only as strong as its weakest link"

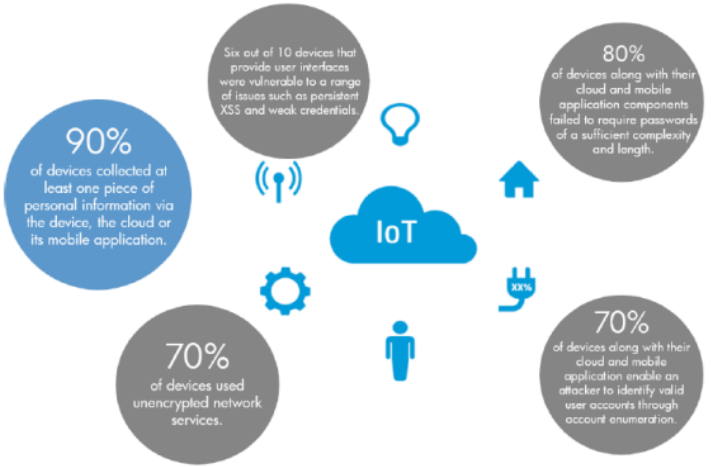
Hackers are increasingly targeting unprotected "internet of things" devices, such as air-conditioning systems and CCTV, to get into corporate networks.

Hackers used a **fish tank** which was **connected to the Internet of Things (IoT)** to get access to a casino's high-roller database.

The attackers used that to get a foothold in the network. They then found the high-roller database and then pulled that back across the network, out the thermostat, and up to the cloud.

IoT Hacks


ATTACK
TAKE CONTROL
STEAL INFORMATION
DISRUPT SERVICES
Controls for smart door locks and lighting systems can be vulnerable.
Door locks have been unlocked remotely.
Infotainment systems offer multiple ways into a car's electronics.
Pacemakers can be attacked remotely.
Personal-fitness devices can tell a hacker where you are.
Malware-infested refrigerators have sent spam.
High-capacity insulin pumps are vulnerable.
Hacked vehicle-control systems can allow remote control of brakes.


Six out of 10 devices that provide user interfaces were vulnerable to a range of issues such as persistent XSS and weak credentials.
80%
of devices along with their cloud and mobile application components failed to require passwords of a sufficient complexity and length.
90%
of devices collected at least one piece of personal information via the device, the cloud or its mobile application.
IoT
70%
of devices used unencrypted network services.
70%
of devices along with their cloud and mobile application enable an attacker to identify valid user accounts through account enumeration.

Case Study: Hackable Cardiac Devices

INNOLYTICS GROUP

The US government has put out an alert over a critical flaw affecting scores of Medtronic heart defibrillators that allows a nearby attacker to change the settings of a patient's cardiac device by manipulating radio communications between it and control devices.

BUSINESS

750,000 Medtronic defibrillators vulnerable to hacking

The Homeland Security Department, which oversees security in critical U.S. infrastructure including medical devices, issued an alert.

By Joe Carlson Star Tribune | MARCH 21, 2019 — 9:38PM

The Medtronic CareLink 2090 Programmer is a portable computer system used to program and manage cardiac devices in clinic and during implant. The device allows a doctor to set the exact parameters for when the defibrillator should send

As many as 750,000 heart devices made by Medtronic PLC contain a serious cybersecurity vulnerability that could let an attacker with sophisticated insider knowledge harm a patient by altering programming on an implanted defibrillator, company and federal officials said Thursday.

TEXT SIZE

43

Mortgage | Credit Cards | Home Equity

Rate	+/-	Last Week	Product
3.112%	▼	3.145%	15-year fixed
3.62%	▼	3.731%	30-year fixed
3.65%	▲	3.648%	3/1 ARM
3.425%	▼	3.446%	5/1 ARM

Rate details
Informa Research Services

View Rates in Your State

Top Stories

Bahamian students come together at St. John's, St. Ben's

1:13am

Global Cybersecurity Spending

INNOLYTICS GROUP

Worldwide Security Spending by Segment, 2017-2019 (Millions of U.S. Dollars)

Market Segment	2017	2018	2019
Application Security	2,434	2,742	3,003
Cloud Security	185	304	459
Data Security	2,563	3,063	3,524
Identity Access Management	8,823	9,768	10,578
Infrastructure Protection	12,583	14,106	15,337
Integrated Risk Management	3,949	4,347	4,712
Network Security Equipment	10,911	12,427	13,321
Other Information Security Software	1,832	2,079	2,285
Security Services	52,315	58,920	64,237
Consumer Security Software	5,948	6,395	6,661
Total	**101,544**	**114,152**	**124,116**

Source: Gartner

According to Cybersecurity Ventures, **global spending** on cybersecurity will exceed **$1 trillion cumulatively** for the 5 year period from **2017-2021.**

Cybersecurity Market

INNOLYTICS GROUP

Total market size in 2019

169,844.99 Million USD

Total market size in 2024

286,198.68Million USD

Average market CAGR

11.0%

Adjacent market sectors

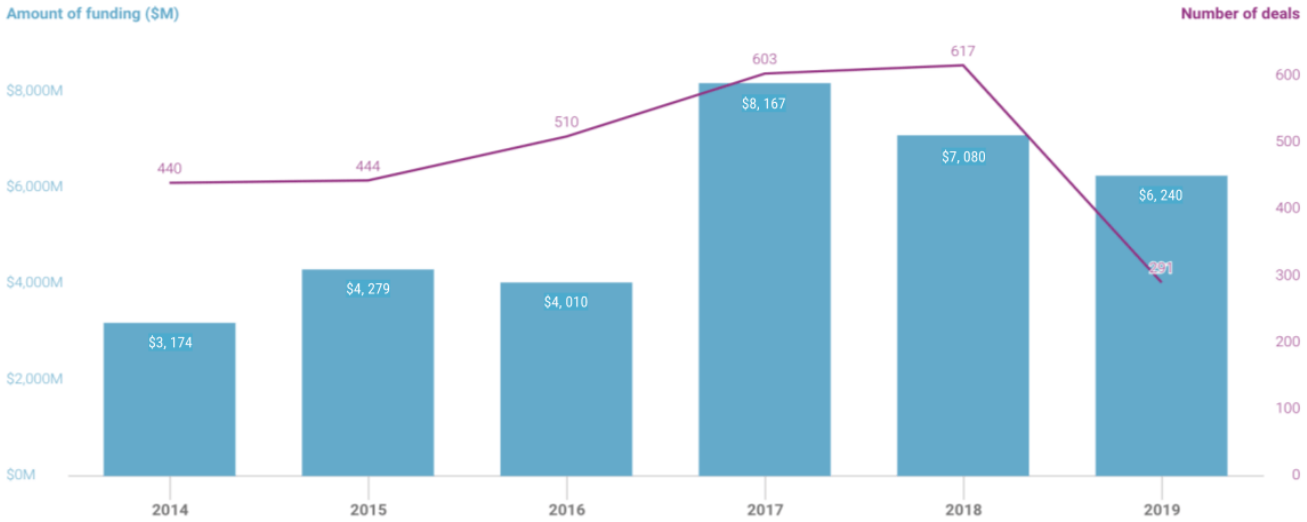
Market Segment	CAGR(%)	2019 (M USD)	2024 (M USD)
Security Analytics (2016-2021)	27.1	5,810.63	19,273.07
Sandboxing (2017-2022)	26.5	4,640.65	15,032.52
Network Forensics (2016-2021)	16.6	1,981.55	4,270.69
Cloud Application Security (2017-2022)	15.1	8,982.15	18,145
Security System Integrators (2017-2022)	8.6	11,510.9	17,388.36

Source:Discovery

Cybersecurity Venture Investment

INNOLYTICS GROUP

Cybersecurity annual global investment activity*



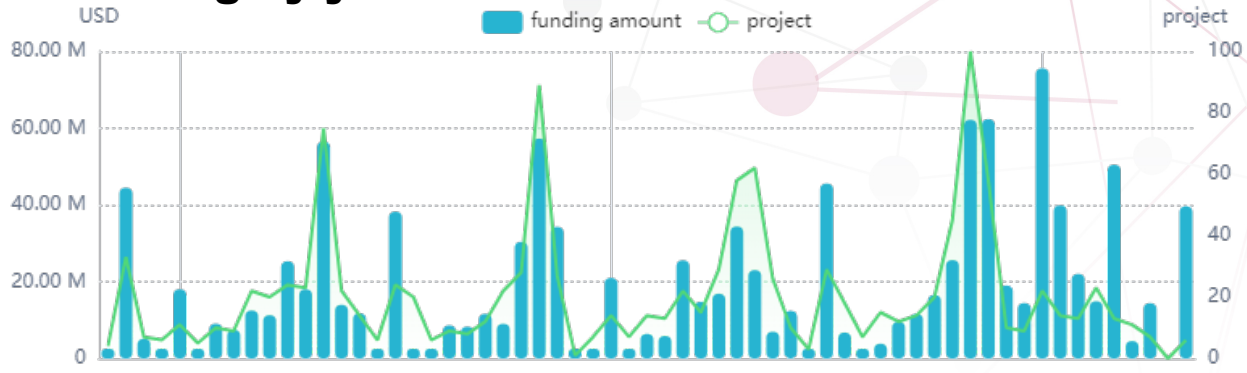
** 2014-2019 (7/12/19)*

Source:CBINSIGHTS

Cybersecurity R&D Funding

INNOLYTICS GROUP

R&D funding by year



Source:Discovery

The biggest R&D projects funded by EC in

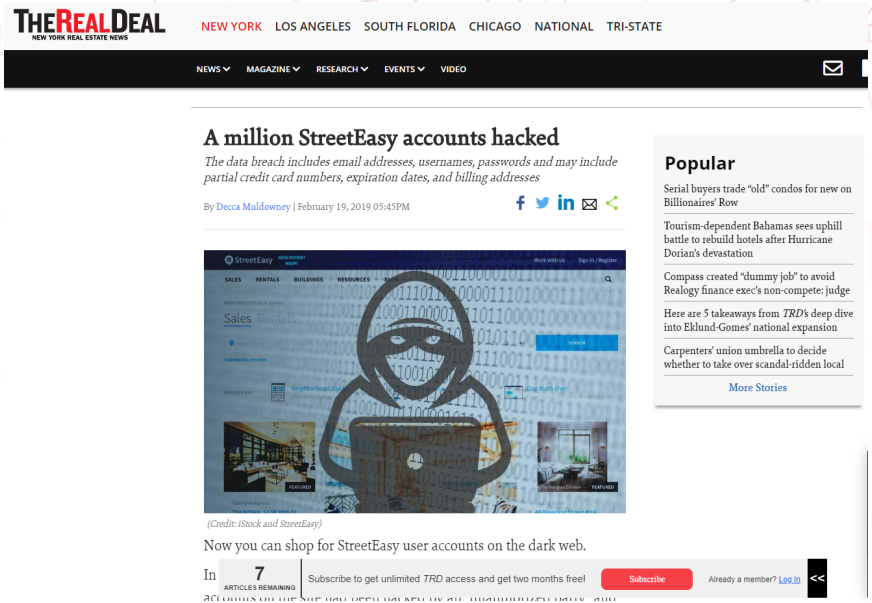
Project funded	Amount (USD)
Cyber Security Network of Competence Centres for Europe	18,353,578
Strategic programs for advanced research and technology in Europe	18,353,500
Cyber security competence for Research and Innovation	18,324,954
Digital Technologies, Advanced Robotics and increased Cyber-security for Agile Production in Future European Manufacturing Ecosystems	18,323,270
European network of Cybersecurity centres and competence Hub for innovation and Operations	18,198,326

Case Study: Street Easy

The company **didn't realize that it had been hacked** until it discovered its **information on sale** in **dark web forums**

According to the spokesperson, the leaked data include:

- Users' full names
- Email Addresses
- Encrypted passwords



THE REAL DEAL
NEW YORK REAL ESTATE NEWS

NEW YORK LOS ANGELES SOUTH FLORIDA CHICAGO NATIONAL TRI-STATE

NEWS MAGAZINE RESEARCH EVENTS VIDEO

A million StreetEasy accounts hacked

The data breach includes email addresses, usernames, passwords and may include partial credit card numbers, expiration dates, and billing addresses

By Decca Muldowney | February 19, 2019 05:45PM

(Credit: iStock and StreetEasy)

Now you can shop for StreetEasy user accounts on the dark web.

In

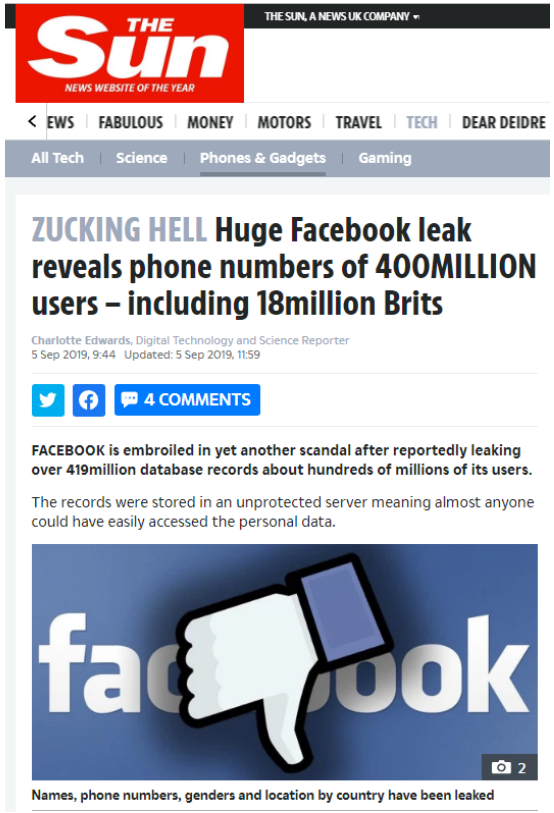
Popular

- Serial buyers trade "old" condos for new on Billionaires' Row
- Tourism-dependent Bahamas sees uphill battle to rebuild hotels after Hurricane Dorian's devastation
- Compass created "dummy job" to avoid Realogy finance exec's non-compete: judge
- Here are 5 takeaways from *TRD*'s deep dive into Eklund-Gomes' national expansion
- Carpenters' union umbrella to decide whether to take over scandal-ridden local

More Stories

Case Study: Another Facebook Information Leak?

INNOLYTICS GROUP



THE Sun
NEWS WEBSITE OF THE YEAR

THE SUN, A NEWS UK COMPANY

EWS | FABULOUS | MONEY | MOTORS | TRAVEL | TECH | DEAR DEIDRE

All Tech | Science | Phones & Gadgets | Gaming

ZUCKING HELL **Huge Facebook leak reveals phone numbers of 400MILLION users – including 18million Brits**

Charlotte Edwards, Digital Technology and Science Reporter
5 Sep 2019, 9:44 Updated: 5 Sep 2019, 11:59

4 COMMENTS

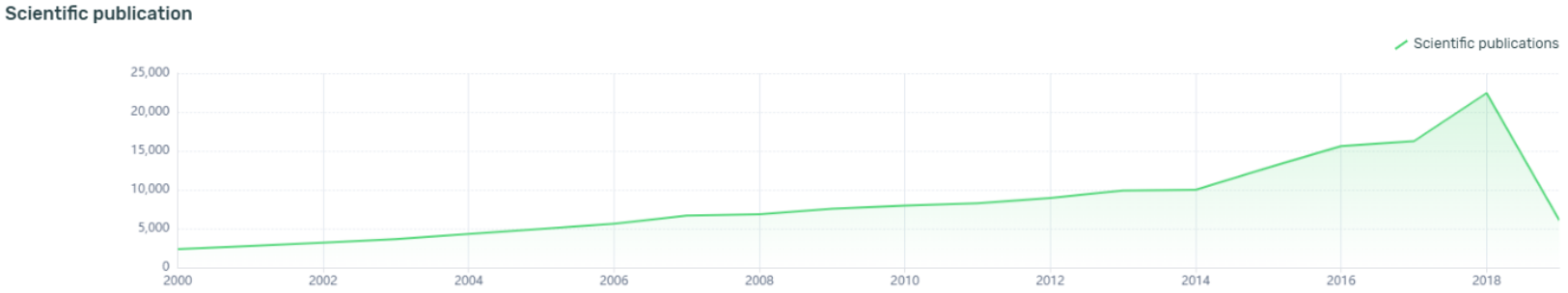
FACEBOOK is embroiled in yet another scandal after reportedly leaking over 419million database records about hundreds of millions of its users.

The records were stored in an unprotected server meaning almost anyone could have easily accessed the personal data.

Names, phone numbers, genders and location by country have been leaked

The exposed server contained more than 419 million records over several databases on users across geographies.
Each record contained a user's unique Facebook ID and the phone number listed on the account.

Cybersecurity scientific publication trend



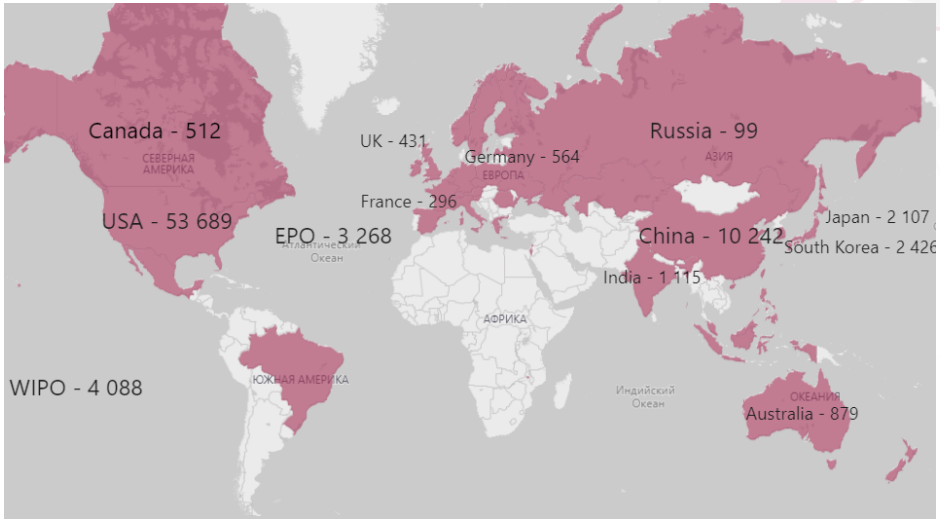
Source: Innolytics Group, Discovery

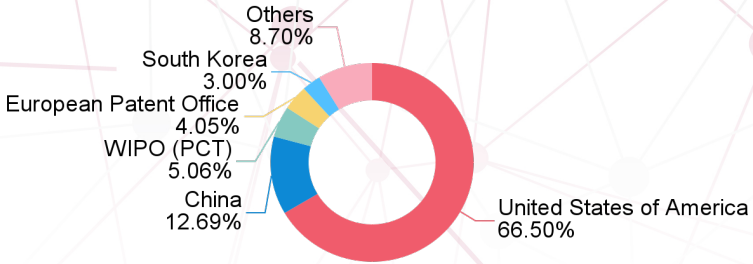
Cybersecurity Patent Landscape Development through Years*

*based on 80,734 simple families

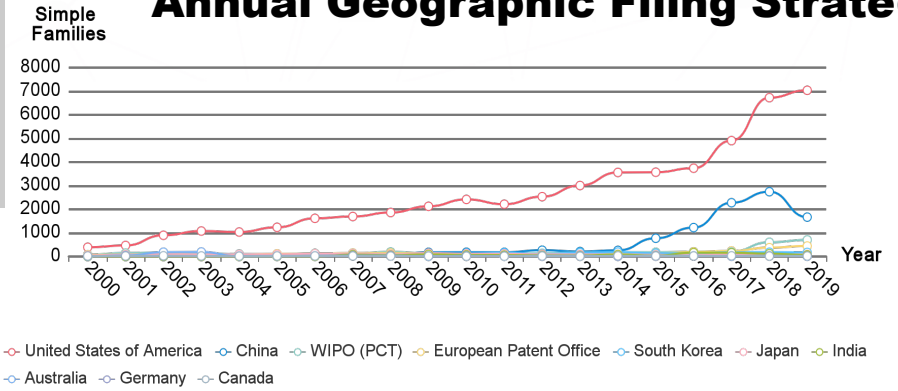
Cybersecurity Patenting Geography

Geographic Territory Map





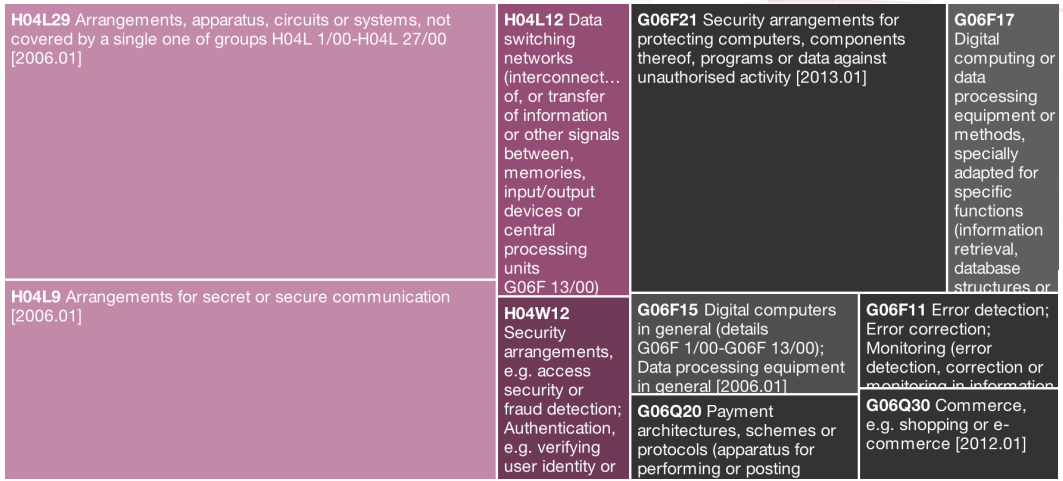
Annual Geographic Filing Strategy



Cybersecurity Technology Focus

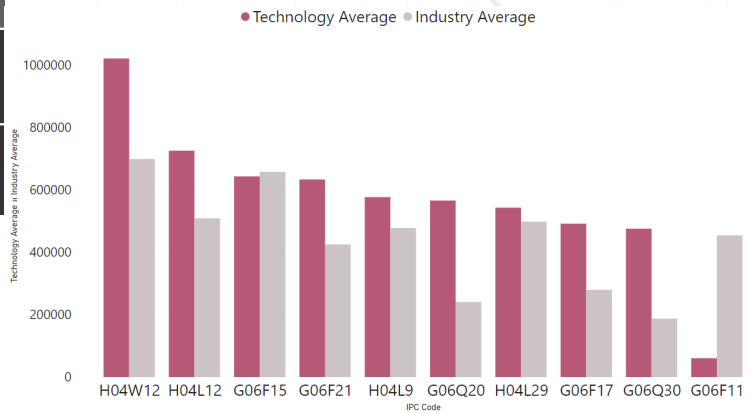
INNOLYTICS GROUP

Top IPC Codes



Technology Area Benchmark

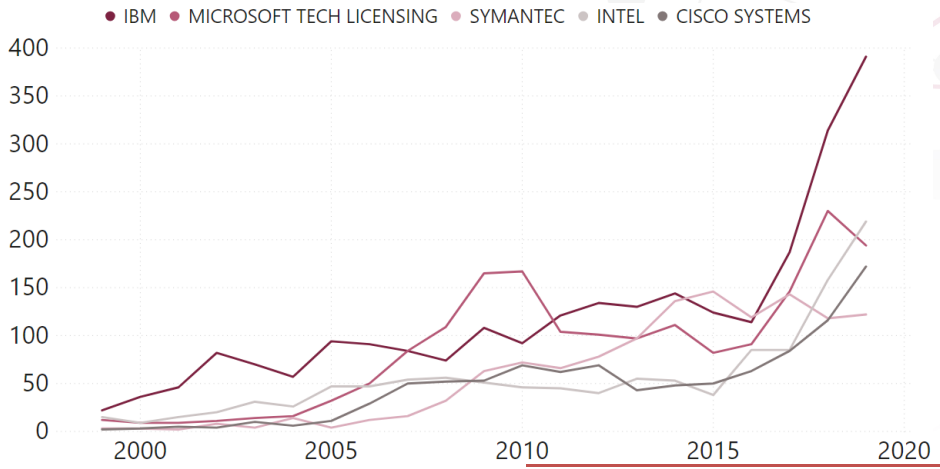
$464,745 Technology Average Patent Value

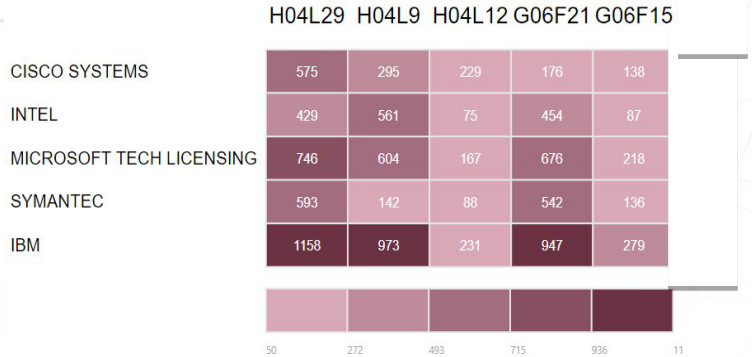


Cybersecurity Main Patent Holders

INNOLYTICS GROUP

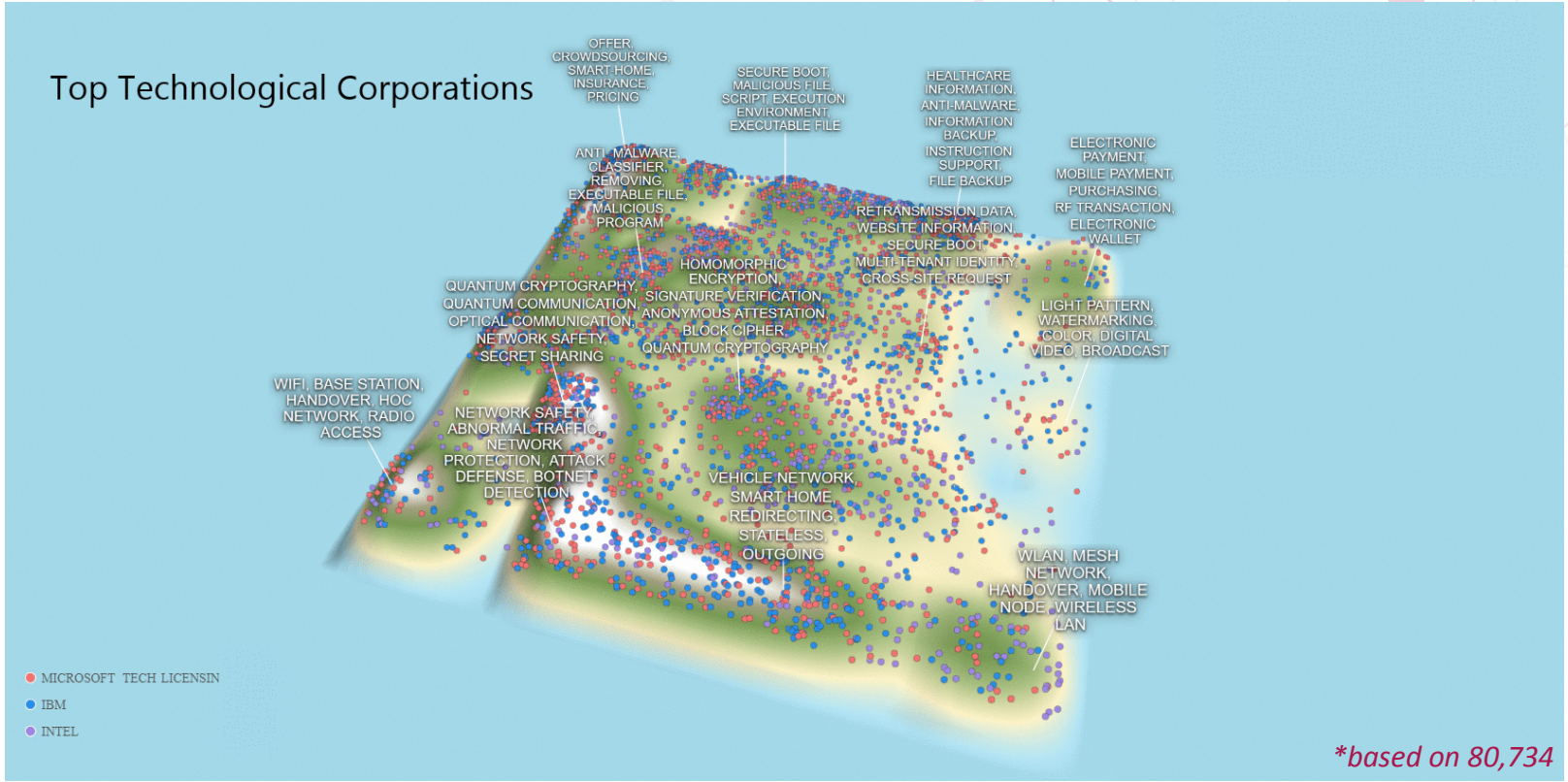
Leaders Technological Focus





H04L29	Arrangements, apparatus, circuits or systems
H04L9	Arrangements for secret or secure communication
H04L12	Data switching networks (interconnection of, or transfer of information or other signals between, memories, input/output devices or central processing units)
G06F21	Security arrangements for protecting computers, components thereof, programs or data against unauthorised activity
G06F15	Digital computers in general; Data processing equipment in general

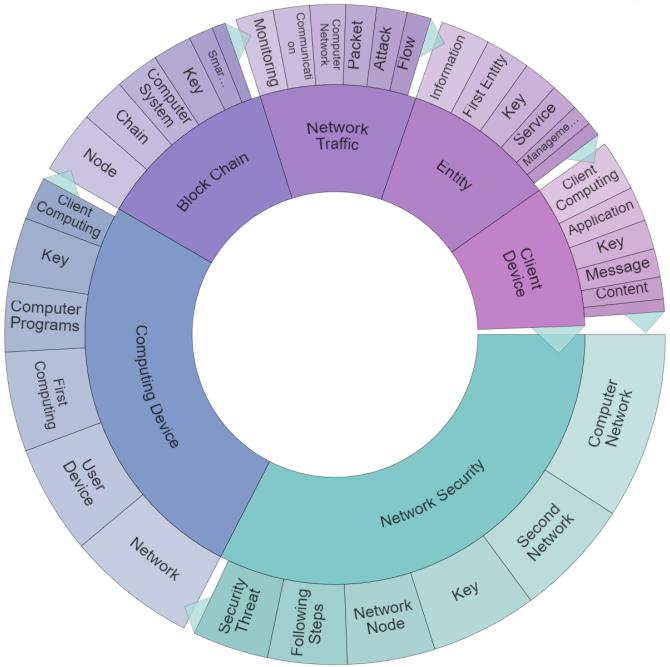
Cybersecurity Main Patent Holders*



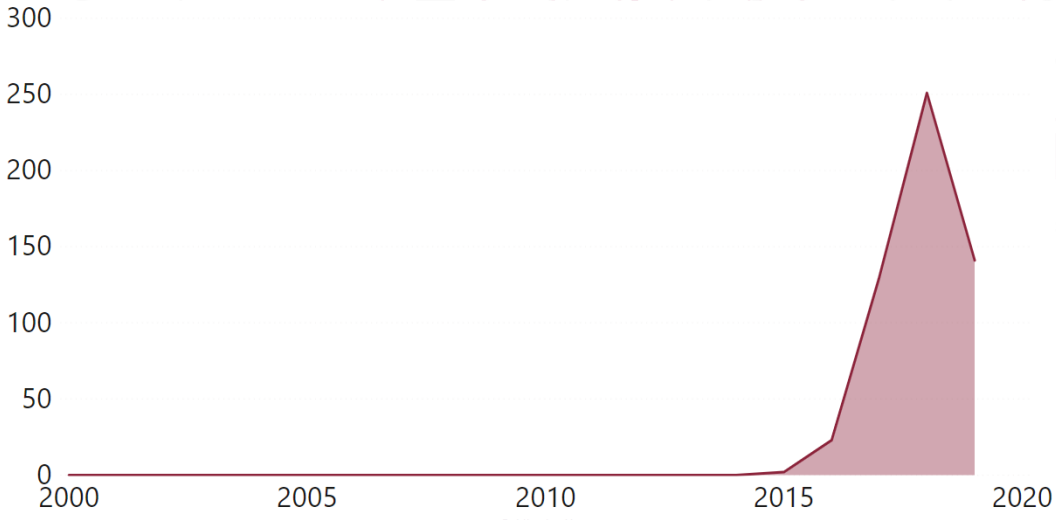
*based on 80,734 simple families

Cybersecurity Elements

Wheel of Innovation



Blockchain in Cybersecurity Patent Activ

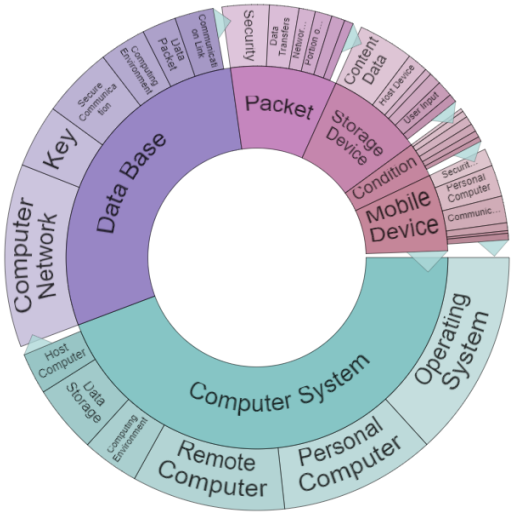


Source: Innolytics Group

Cybersecurity Litigation Cases

Total Cases	Ave. Duration (US only)	Patents Involved	Plaintiff	Defendants
2,216	20.7 mths	913	622	1,460

Litigated Concepts



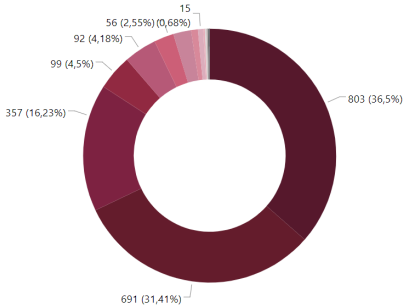
Top 3 Most Aggressive Plaintiffs

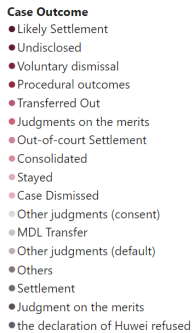
Blue Spike Inc
73 cases

Cryptopeak Solutions LLC
66 cases

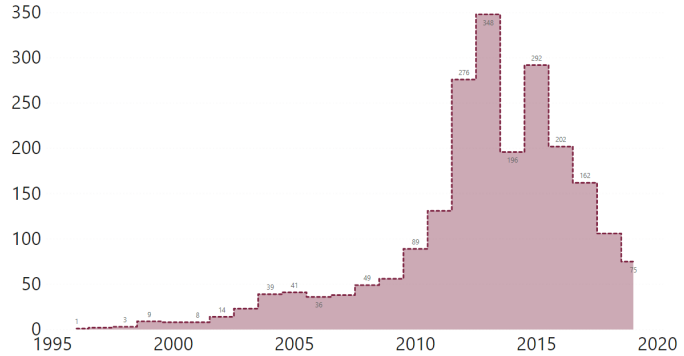
Uniloc USA Inc
63 cases

Case Outcomes





Litigation Timeline



Litigation Case of Highest Market-Valued Patent

US7895641 Method and system for dynamic network intrusion monitoring, detection and response (2011) $ 2,010,000

Plaintiff *British Telecommunications Plc*

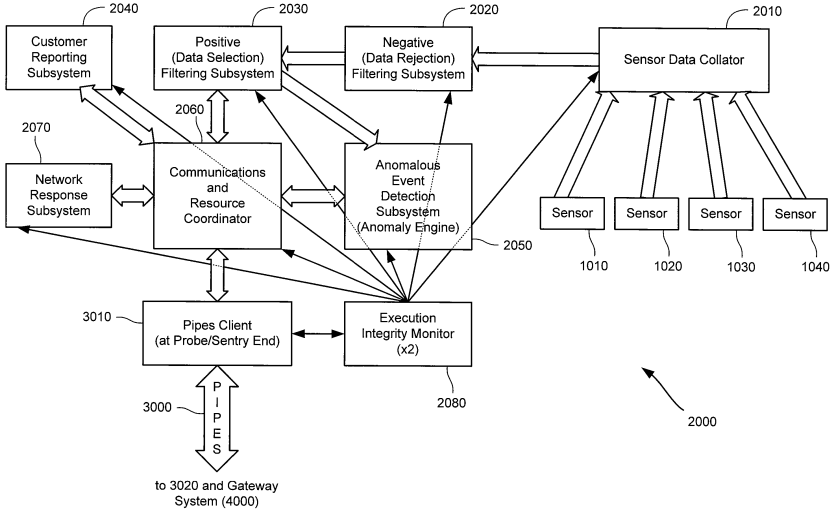
BT Americas Inc.

Defendant *Fortinet Inc.*

Products: FortiGate, FortiWeb, FortiMail, FortiSandbox, FortiManager, FortiAnalyzer, FortiGuard - Network security monitoring systems

Patens Involved: US7693971, US7370358, US7895641, US7774845, US7159237

*This invention relates generally to **network security** and, more specifically, to methods and systems for dynamic network intrusion monitoring, detection and response.*



Fortinet Inc - Perennial Defendant

INNOLYTICS GROUP

Fortinet, Inc. provides network security solutions. The Company offers network security appliances, related software, and subscription services.

Fortinet Inc. is defendant in

81 Litigation Cases

Total company's patent portfolio includes

306 patent families

Example of Patent Dispute Settlement

INNOLYTICS GROUP

US9356948 Collaborative phishing attack detection $ 1,090,000

Plaintiff
PhishMe Inc.

Defendant
Wombat Security Technologies Inc.

Products: cybersecurity software products, services

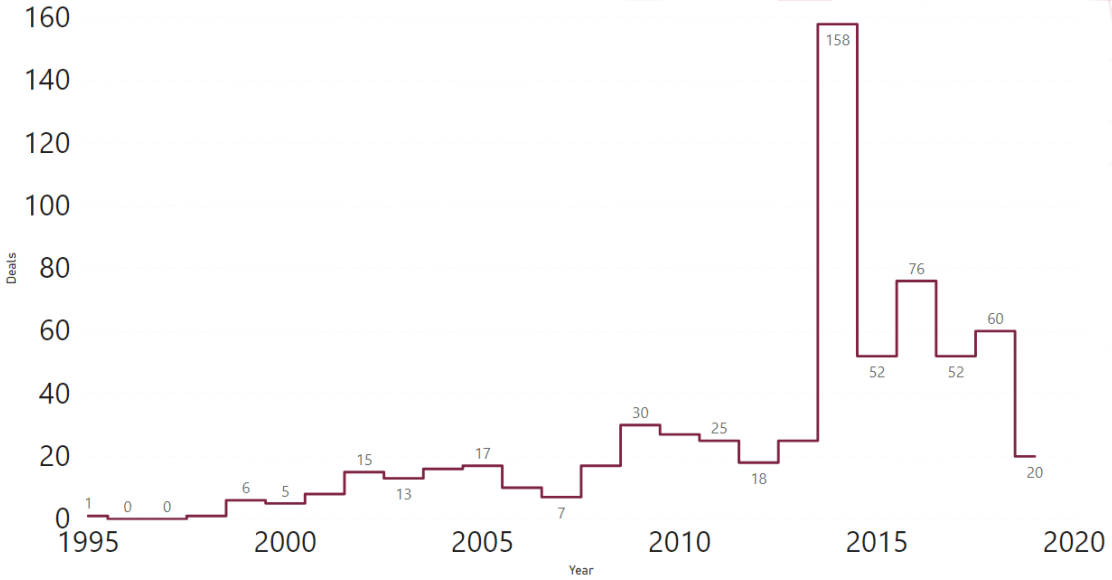
*Described herein are methods, network devices and machine-readable storage media for **detecting** whether a message is a **phishing attack** based on the collective responses from one or more individuals who have received that message.*

PhishMe Inc. and **Wombat Security Technologies Inc.** have settled their patent dispute and entered into an agreement resolving the claims at issue in the litigation.

As a part of the settlement, **PhishMe granted a license** to **Wombat** to the PhishMe patents involved in the litigation.

Cybersecurity Patents Licencing

Annual In-Licensing and Out-Licensing Timeline



Top 3 Licensers

Inventor HLDG	13 licenses
Nanjing University of Posts & Telecommunications	13 licenses
Walker Digital	13 licenses

Cybersecurity Most Valuable Patents*

Total Value	Min Total Value	Max Total Value	Simple Family Numbers
$26,730,746,600 (USD)	$19,235,483,400 (USD)	$34,234,865,000 (USD)	57,517

Top Most Valuable patents

Patent/Title	Value (USD)	Assignee
US10028144 Security techniques for device assisted services	$82,930,000	HEADWATER RES LLC
US20180167963A1 Communication of security key information	$45,360,000	INTEL IP
US9426689 Control and data plane solutions for carrier-aggregation based WLAN offload	$40,830,000	INTEL

*based on 80,734 simple families

Cybersecurity Most Valuable Patent with Ukrainian Inventor

INNOLYTICS

US20180241727A1 Secure Dynamic Communication Network And Protocol (2018)

$ 1,040,000

*In a **secure cloud** for transmitting packets of digital data, the packets may be repeatedly scrambled (i.e., their data segments reordered) and then unscrambled, split and then mixed, and/or encrypted and then decrypted as they pass through media nodes in the cloud.*

*The methods used to scramble, split, mix and encrypt the packets may be varied in accordance with a state such as time, thereby making the **task of a hacker virtually impossible** inasmuch as he or she may be viewing only a fragment of a packet and the methods used to disguise the data are constantly changing.*

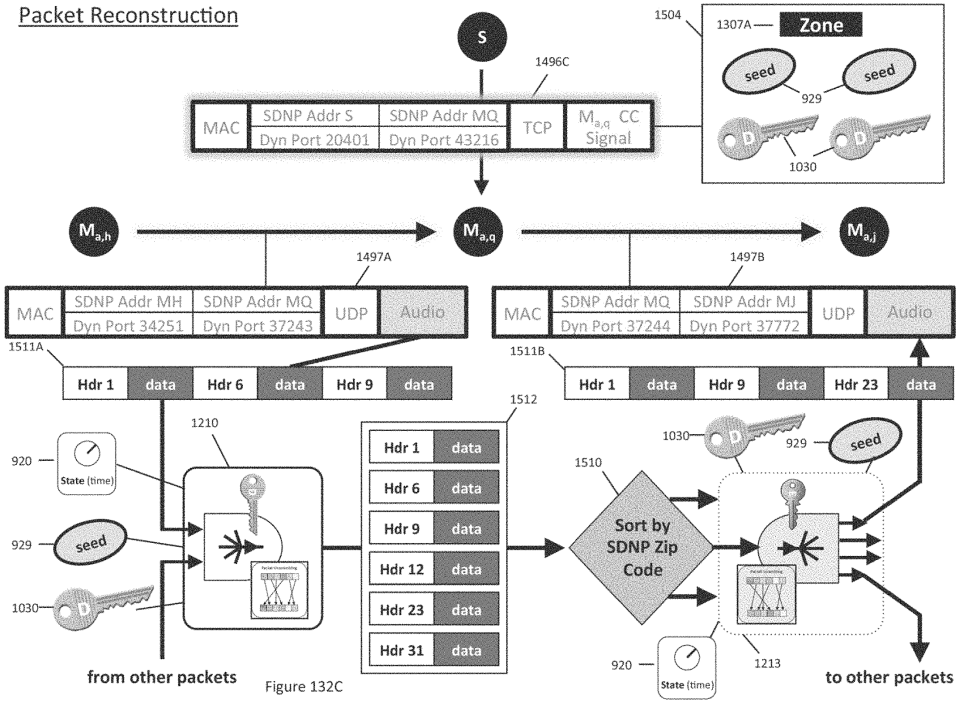
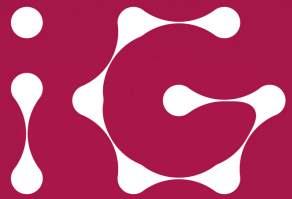


Figure 132C



INNOLYTICS
GROUP

www.innolyticsgroup.com