IBM Security Strategy
Fearless in the face of uncertainty

—

Kenneth Gonzalez – IBM X-Force Red
Javier Portuguez – IBM Security Eng.

IBM **Security**

Cybersecurity is a universal challenge

What's at stake...

20.8 billion
things we need
to secure

5 billion
personal data
records stolen

$6 trillion
lost to cybercrime
over the next 2 years

What we face...

Compliance updates

GDPR fines can cost
billions
for large global
companies

Skills shortage

By 2022, CISOs will face
1.8 million
unfulfilled
cybersecurity jobs

Too many tools

Organizations are using
too many
tools from too
many vendors

What we’re hearing from customers

Help me…

- Modernize security frameworks and controls
- Respond to the global security skills shortage
- Address increasing cyber attack vectors including IoT
- Maintain data privacy and regulatory compliance
- Secure the journey to cloud and digital transformation

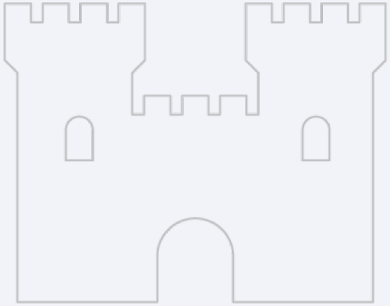
The future of security

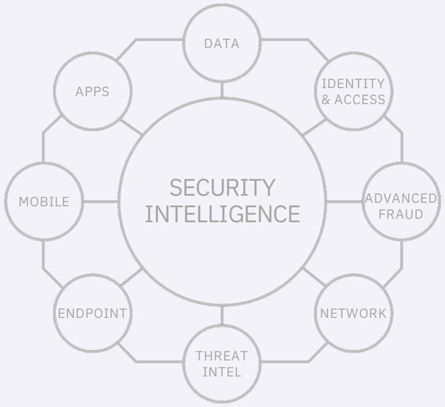
Before 2011
Bolt-on security
for IT projects

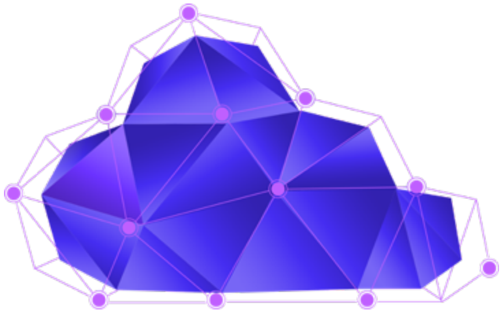
2011-2018
Security intelligence
across the enterprise

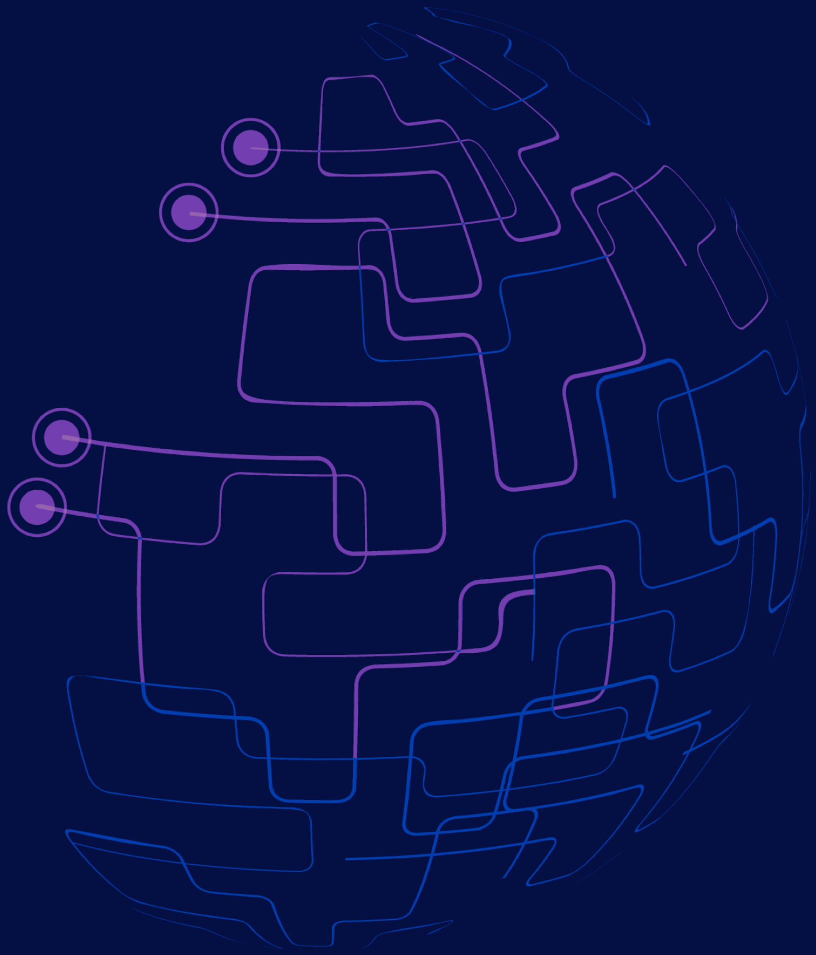
2019+
Connected security for all,
at the “speed of cloud”

Beyond...
AI, quantum, blockchain
and IoT security









Ready for future battles

Thousands of IBM Researchers in 12 labs across 6 continents are busy working on security projects that will shape our future

Good AI versus bad

IBM researchers are finding ways to address the weaknesses found in AI systems

Blockchain for security

IBM invented the way to share threat intelligence that's anonymous and trusted

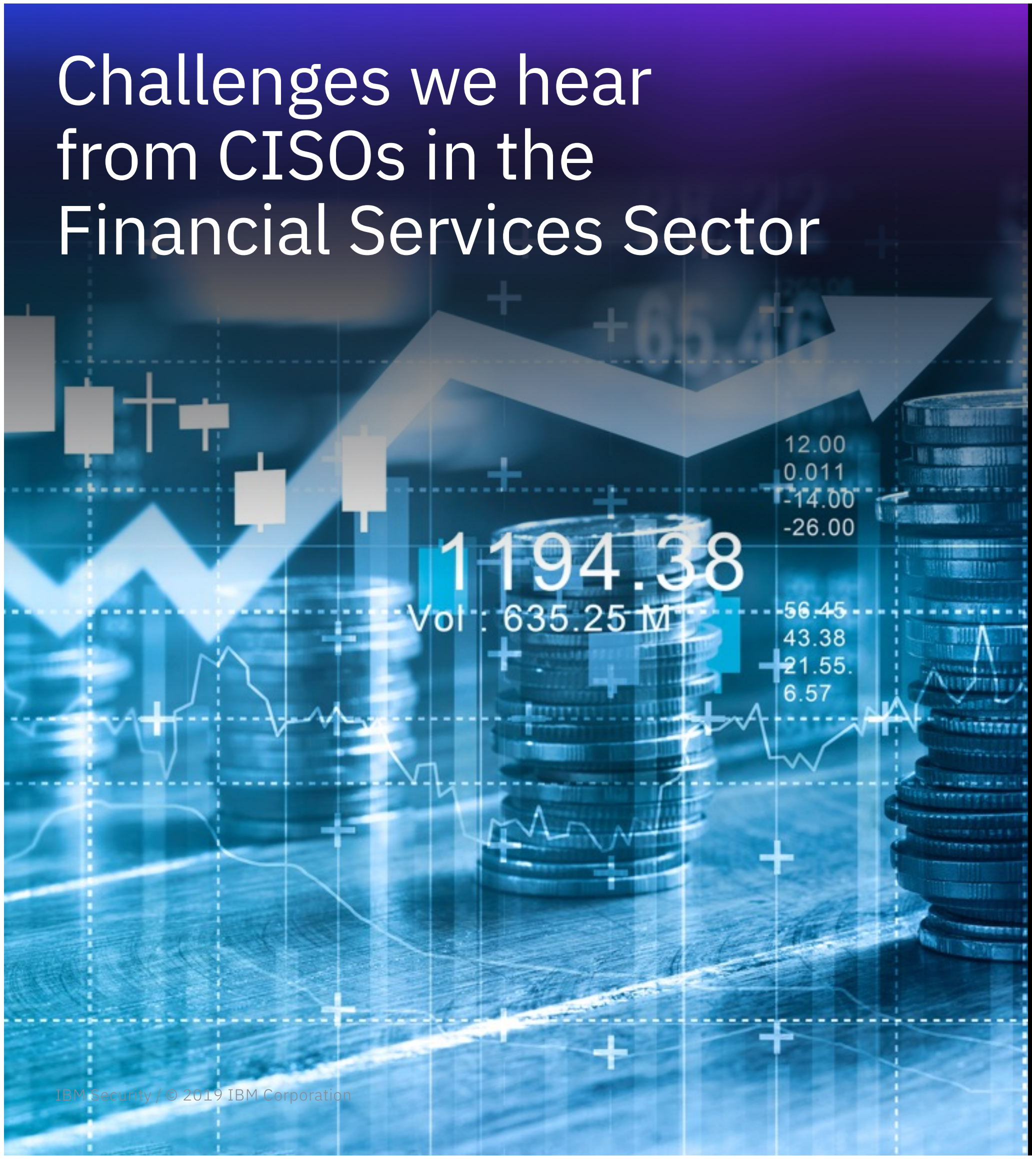
Post-quantum cryptography

Lattice cryptography will protect organizations from quantum-enabled hackers

Securing the world of things

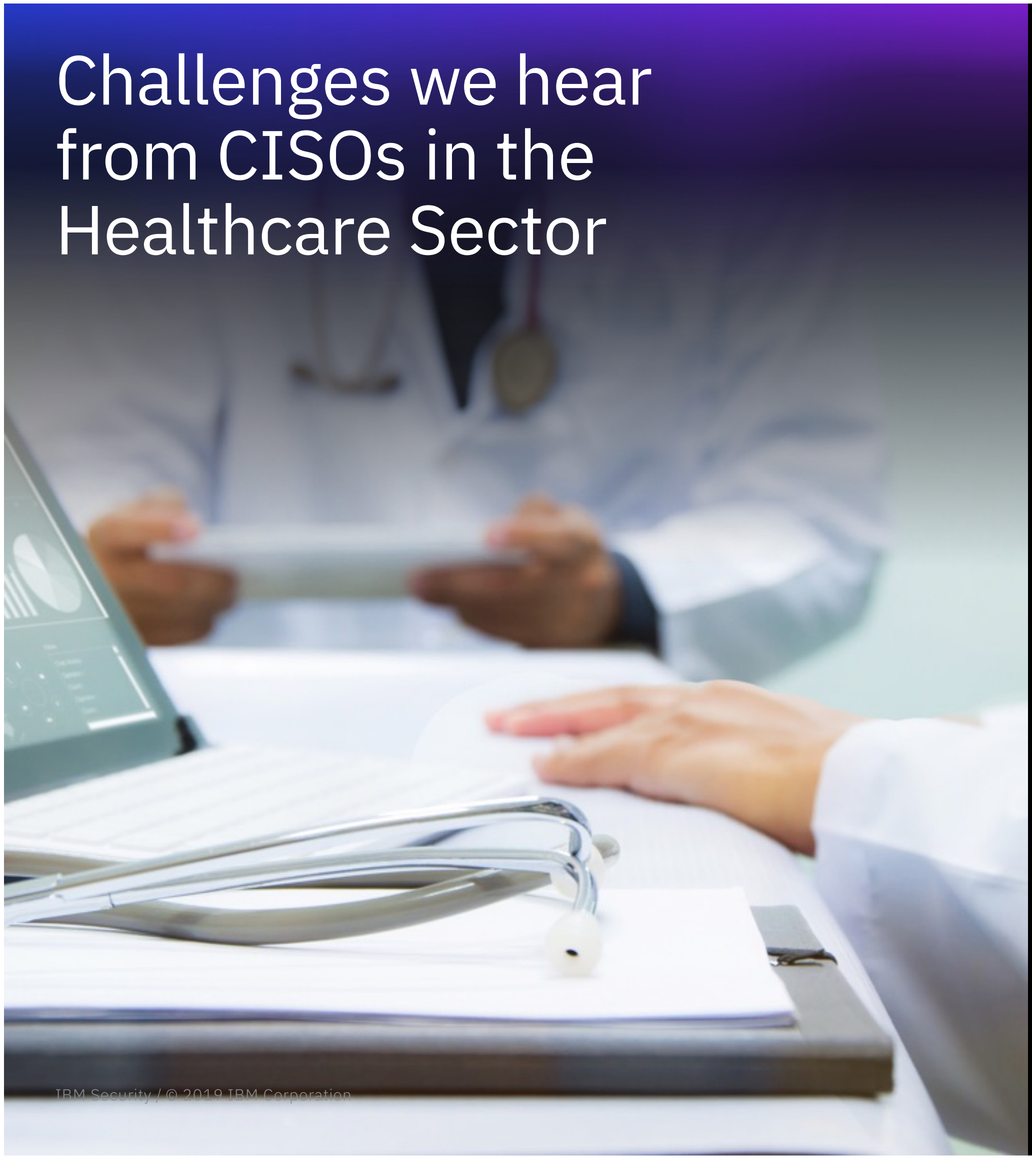
IBM researchers are working on cryptographic algorithms and protocols, and key management to enable end-to-end IoT security

Challenges we hear from CISOs in the Financial Services Sector



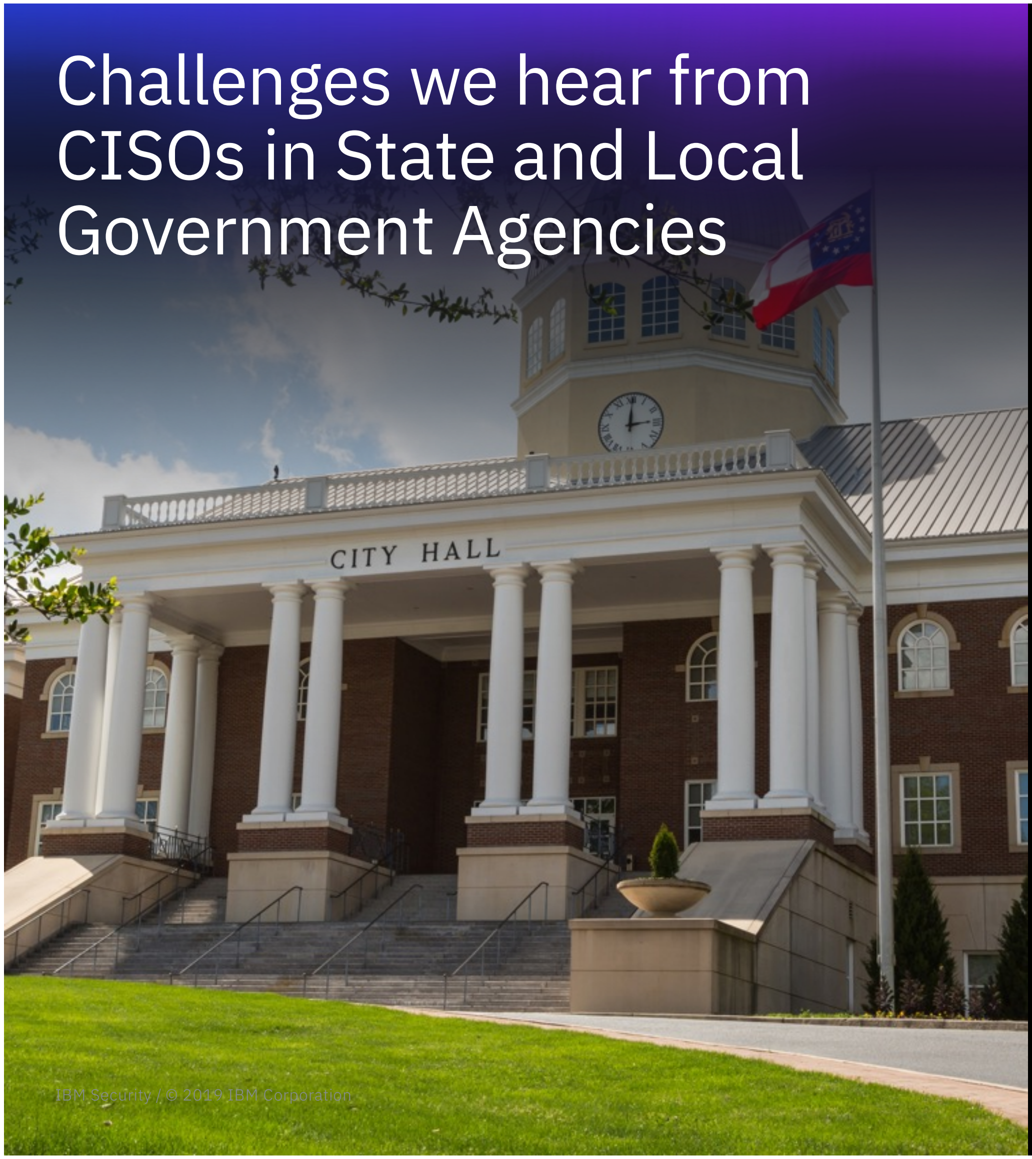
- Focus on regulatory compliance
- Ensure workloads in the cloud meet new security standards
- Increase investments for “right side of the boom”
- Adopt standard security frameworks and controls
- Design integrated risk, compliance and security analytics

Challenges we hear from CISOs in the Healthcare Sector



- Ensure patient privacy, safety and security
- Secure medical devices, sensors and IoT endpoints
- Meet the demands of digital transformation
- Maintain regulatory compliance
- Secure medical images

Challenges we hear from CISOs in State and Local Government Agencies



- Deal with aging infrastructures
- Address insufficient IT administration
- Meet the demands of digital transformation
- Ensure data privacy and compliance
- Respond to talent and funding shortage

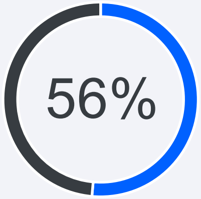
Some numbers

1 of 10 URL's are malicious

In 2018, 1 in 10 URLs analyzed were identified as being malicious, up from 1 in 16 in 2017.

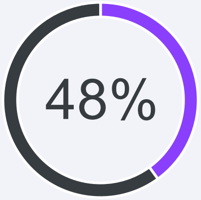
Increase of web attacks

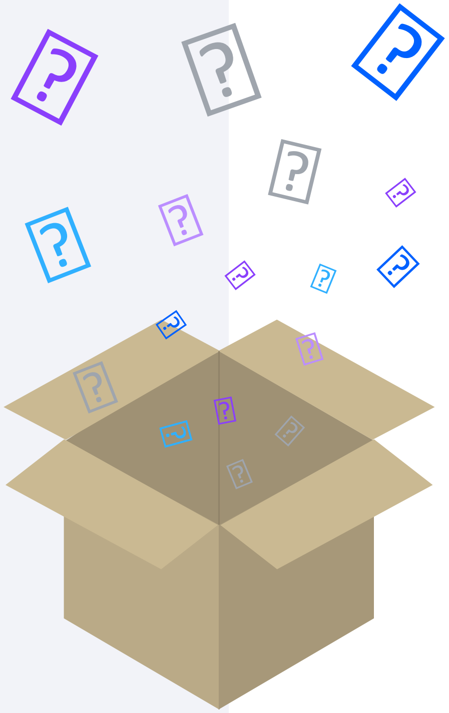
Most of the business have web presence… that's why year by year the web attacks increase their numbers

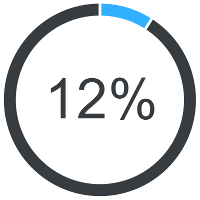


Malicious Emails

Best and preferred way to infect computers, networks and companies with malware

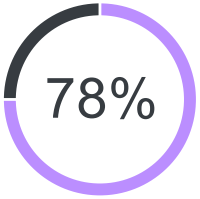






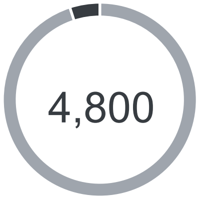
Ransomware

While overall ransomware infections were down, enterprise infections were up by 12 percent in 2018.



Supply Chain Attacks

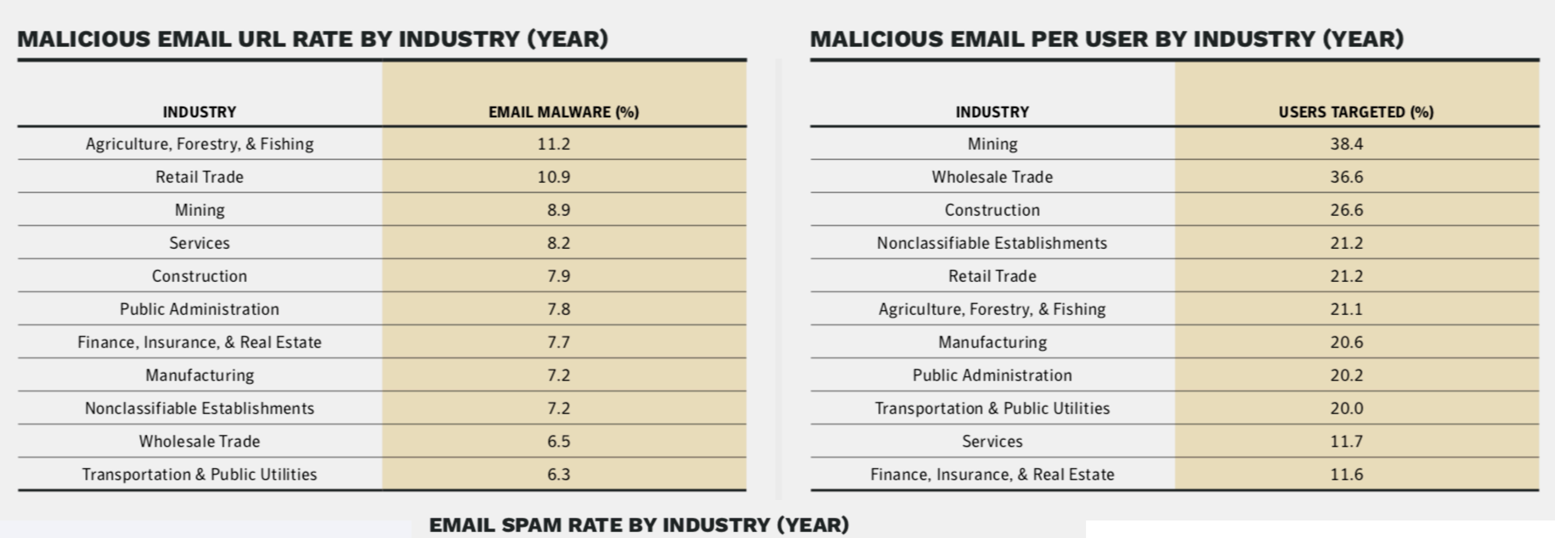
take many forms, including hijacking software updates and injecting malicious code into legitimate software



Formjacking

Use of malicious JavaScript code to steal credit card details and other information from payment forms on the checkout web pages of eCommerce sites

https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf

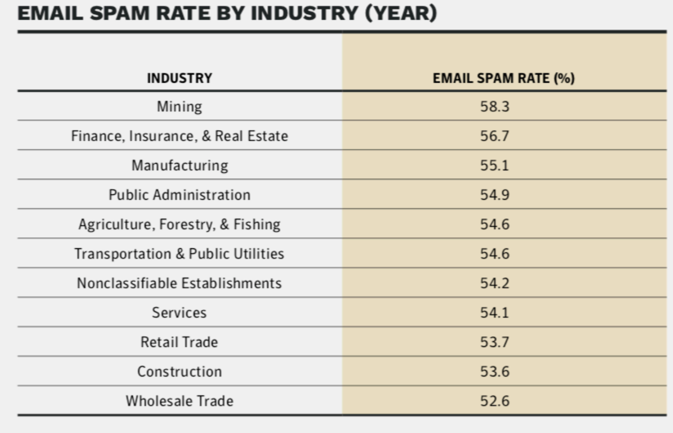


MALICIOUS EMAIL URL RATE BY INDUSTRY (YEAR)

INDUSTRY	EMAIL MALWARE (%)
Agriculture, Forestry, & Fishing	11.2
Retail Trade	10.9
Mining	8.9
Services	8.2
Construction	7.9
Public Administration	7.8
Finance, Insurance, & Real Estate	7.7
Manufacturing	7.2
Nonclassifiable Establishments	7.2
Wholesale Trade	6.5
Transportation & Public Utilities	6.3

MALICIOUS EMAIL PER USER BY INDUSTRY (YEAR)

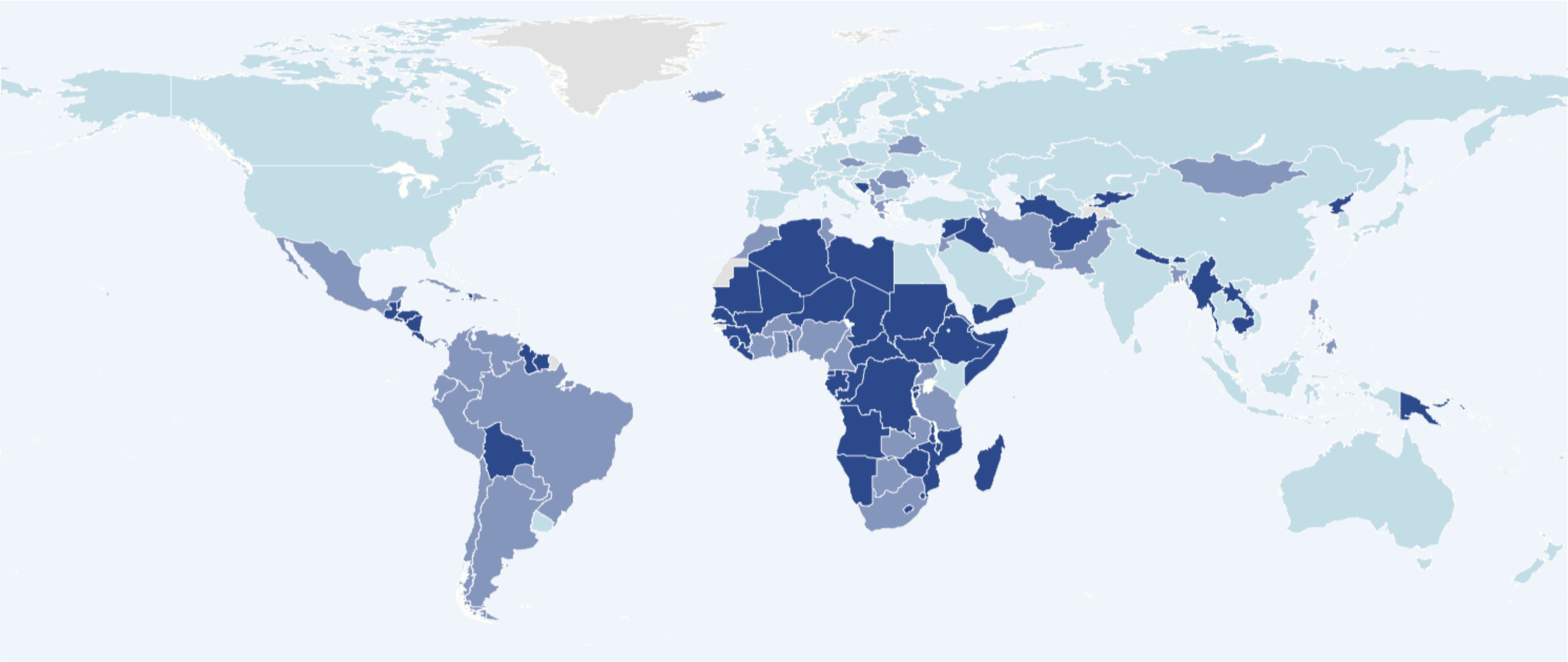
INDUSTRY	USERS TARGETED (%)
Mining	38.4
Wholesale Trade	36.6
Construction	26.6
Nonclassifiable Establishments	21.2
Retail Trade	21.2
Agriculture, Forestry, & Fishing	21.1
Manufacturing	20.6
Public Administration	20.2
Transportation & Public Utilities	20.0
Services	11.7
Finance, Insurance, & Real Estate	11.6

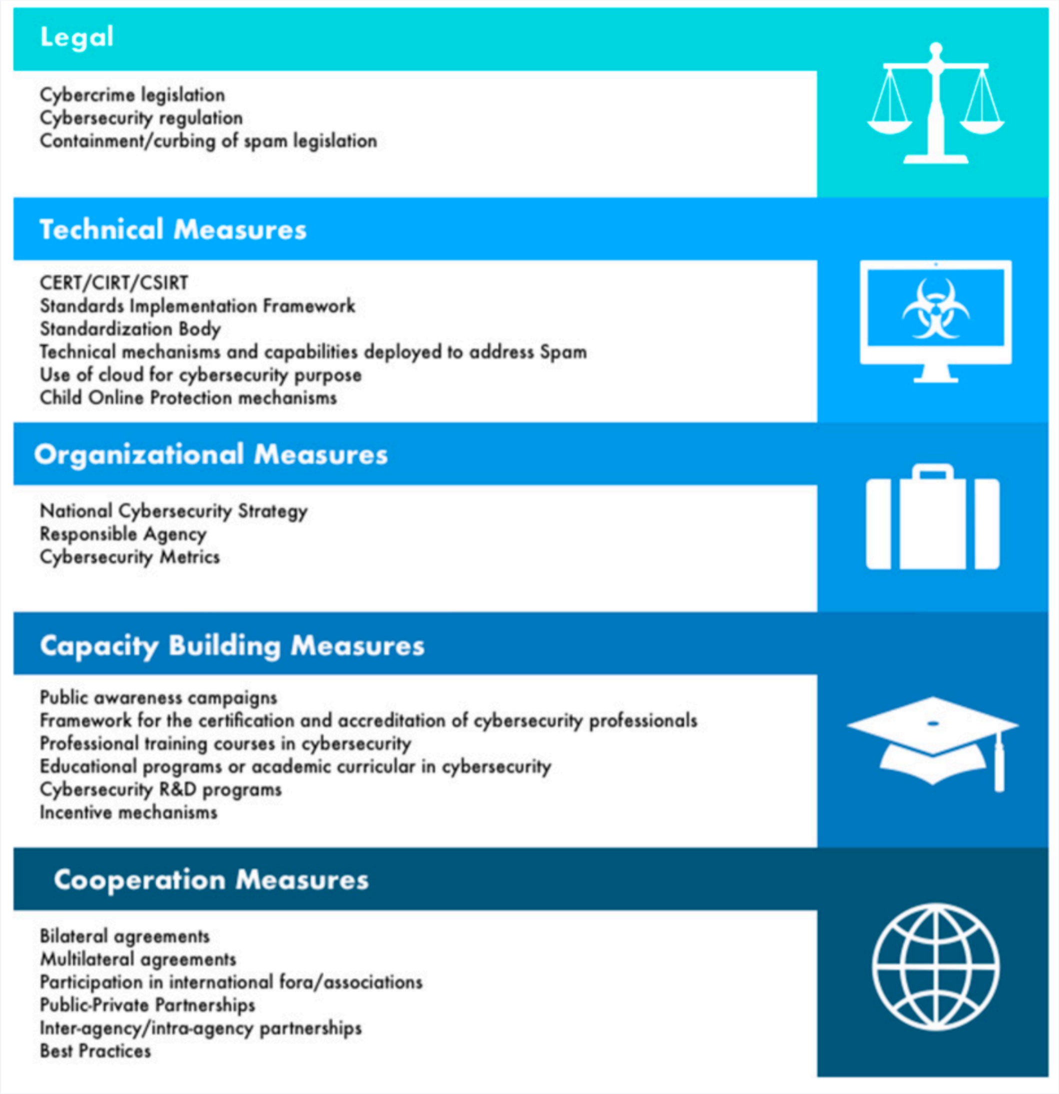


EMAIL SPAM RATE BY INDUSTRY (YEAR)

INDUSTRY	EMAIL SPAM RATE (%)
Mining	58.3
Finance, Insurance, & Real Estate	56.7
Manufacturing	55.1
Public Administration	54.9
Agriculture, Forestry, & Fishing	54.6
Transportation & Public Utilities	54.6
Nonclassifiable Establishments	54.2
Services	54.1
Retail Trade	53.7
Construction	53.6
Wholesale Trade	52.6

Member State	Score	Regional Rank	Global Rank
Costa Rica*	0.221	18	115





Legal

Cybercrime legislation
Cybersecurity regulation
Containment/curbing of spam legislation

Technical Measures

CERT/CIRT/CSIRT
Standards Implementation Framework
Standardization Body
Technical mechanisms and capabilities deployed to address Spam
Use of cloud for cybersecurity purpose
Child Online Protection mechanisms

Organizational Measures

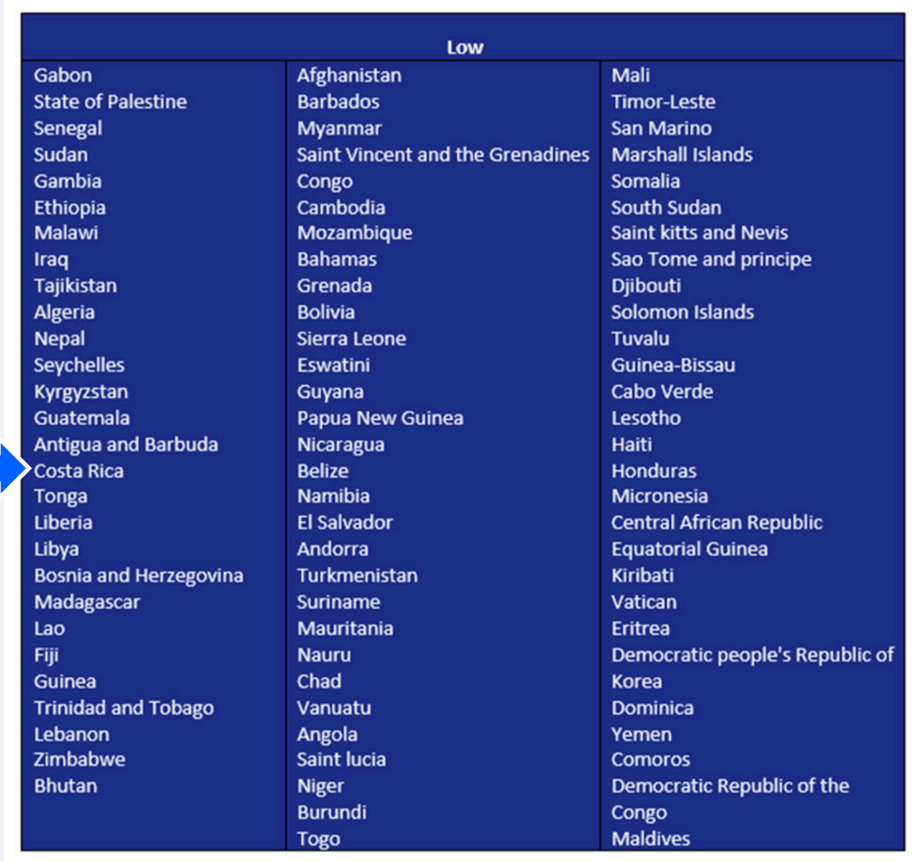
National Cybersecurity Strategy
Responsible Agency
Cybersecurity Metrics

Capacity Building Measures

Public awareness campaigns
Framework for the certification and accreditation of cybersecurity professionals
Professional training courses in cybersecurity
Educational programs or academic curricular in cybersecurity
Cybersecurity R&D programs
Incentive mechanisms

Cooperation Measures

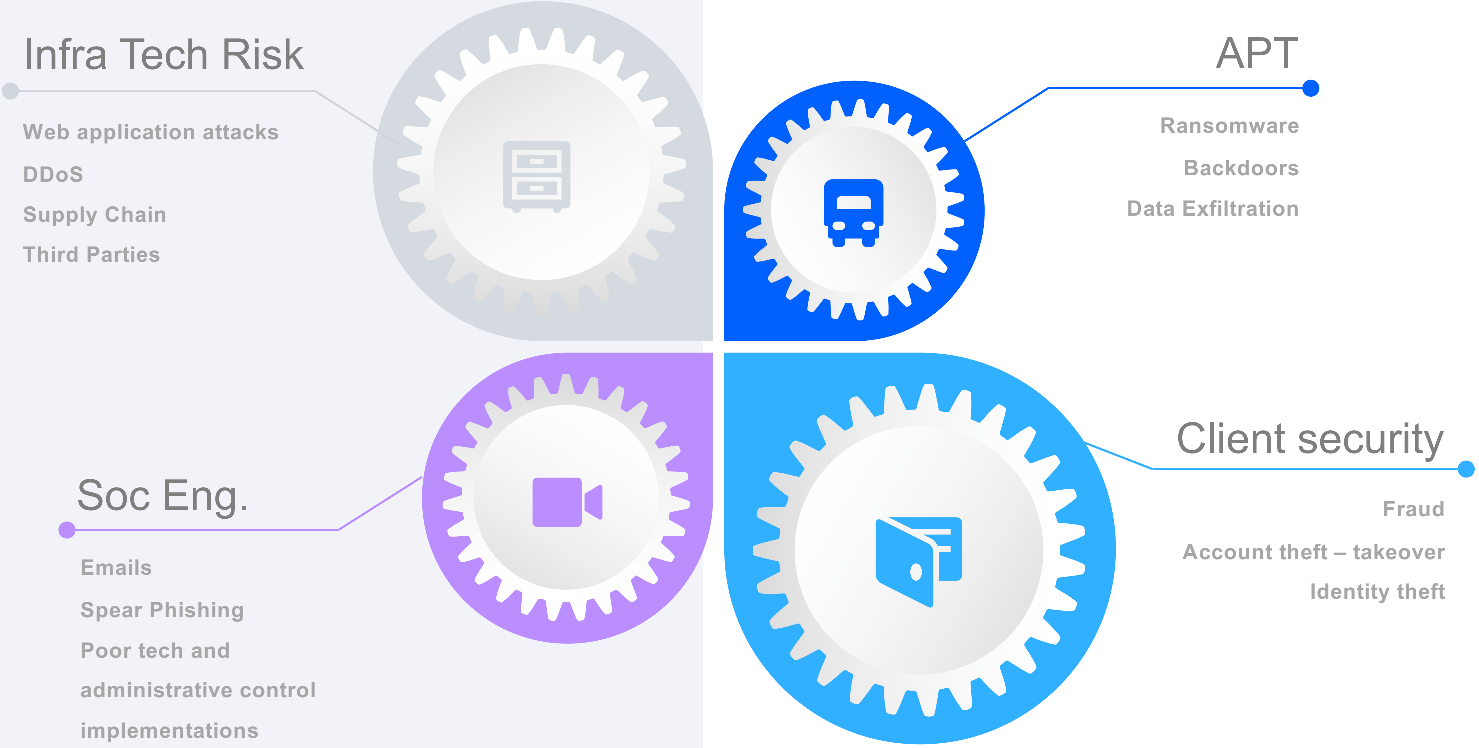
Bilateral agreements
Multilateral agreements
Participation in international fora/associations
Public-Private Partnerships
Inter-agency/intra-agency partnerships
Best Practices



Low		
Gabon State of Palestine Senegal Sudan Gambia Ethiopia Malawi Iraq Tajikistan Algeria Nepal Seychelles Kyrgyzstan Guatemala Antigua and Barbuda Costa Rica Tonga Liberia Libya Bosnia and Herzegovina Madagascar Lao Fiji Guinea Trinidad and Tobago Lebanon Zimbabwe Bhutan	Afghanistan Barbados Myanmar Saint Vincent and the Grenadines Congo Cambodia Mozambique Bahamas Grenada Bolivia Sierra Leone Eswatini Guyana Papua New Guinea Nicaragua Belize Namibia El Salvador Andorra Turkmenistan Suriname Mauritania Nauru Chad Vanuatu Angola Saint lucia Niger Burundi Togo	Mali Timor-Leste San Marino Marshall Islands Somalia South Sudan Saint kitts and Nevis Sao Tome and principe Djibouti Solomon Islands Tuvalu Guinea-Bissau Cabo Verde Lesotho Haiti Honduras Micronesia Central African Republic Equatorial Guinea Kiribati Vatican Eritrea Democratic people's Republic of Korea Dominica Yemen Comoros Democratic Republic of the Congo Maldives

Emerging Cybersecurity Threats

On financial & insurance services



Infra Tech Risk

- Web application attacks
- DDoS
- Supply Chain
- Third Parties

APT

- Ransomware
- Backdoors
- Data Exfiltration

Soc Eng.

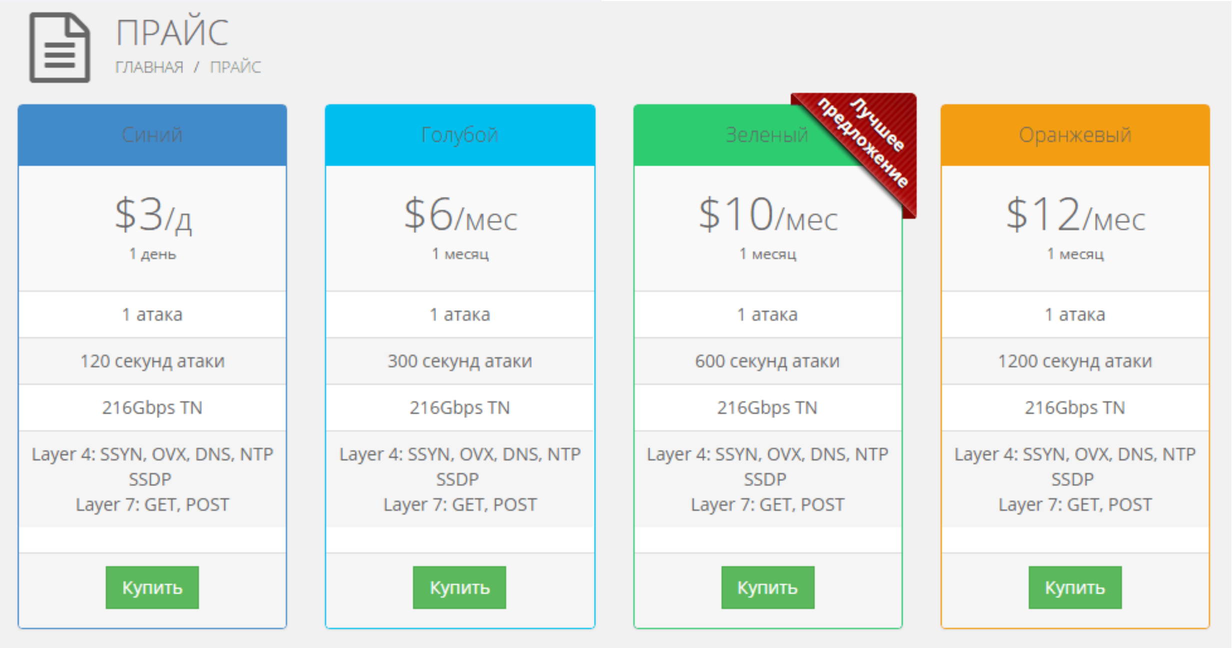
- Emails
- Spear Phishing
- Poor tech and administrative control implementations

Client security

- Fraud
- Account theft – takeover
- Identity theft

Emerging Cybersecurity Threats

Infrastructure technology risk



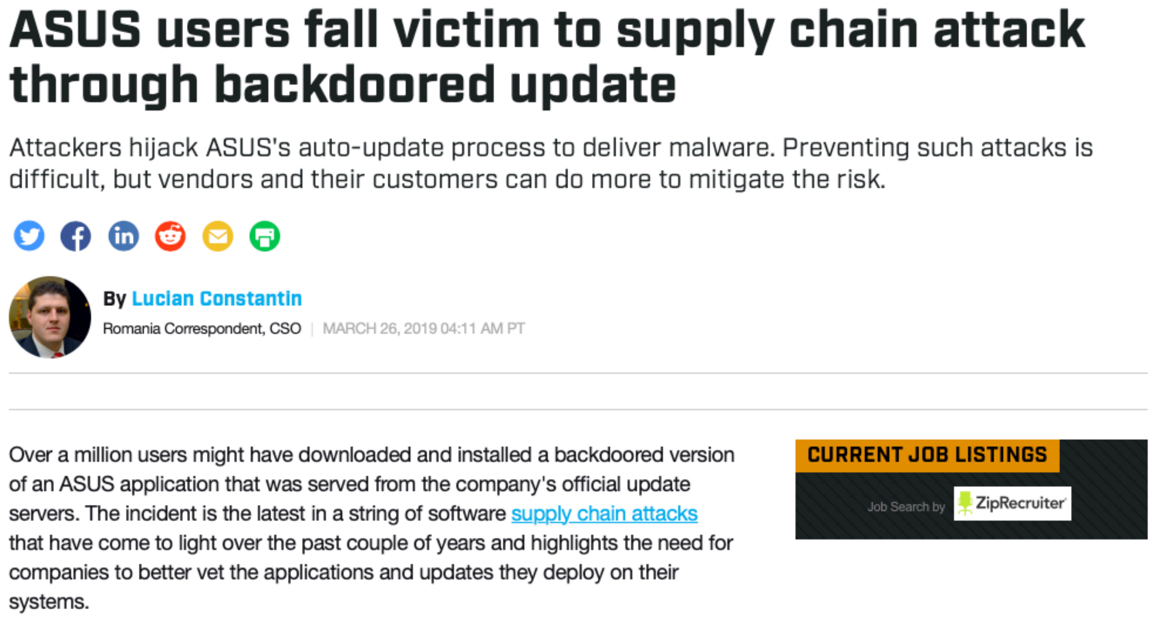
ПРАЙС

ГЛАВНАЯ / ПРАЙС

Синий	Голубой	Зеленый	Оранжевый
		Лучшее предложение	
$3/д	$6/мес	$10/мес	$12/мес
1 день	1 месяц	1 месяц	1 месяц
1 атака	1 атака	1 атака	1 атака
120 секунд атаки	300 секунд атаки	600 секунд атаки	1200 секунд атаки
216Gbps TN	216Gbps TN	216Gbps TN	216Gbps TN
Layer 4: SSYN, OVX, DNS, NTP SSDP Layer 7: GET, POST	Layer 4: SSYN, OVX, DNS, NTP SSDP Layer 7: GET, POST	Layer 4: SSYN, OVX, DNS, NTP SSDP Layer 7: GET, POST	Layer 4: SSYN, OVX, DNS, NTP SSDP Layer 7: GET, POST

Emerging Cybersecurity Threats

Infrastructure technology risk



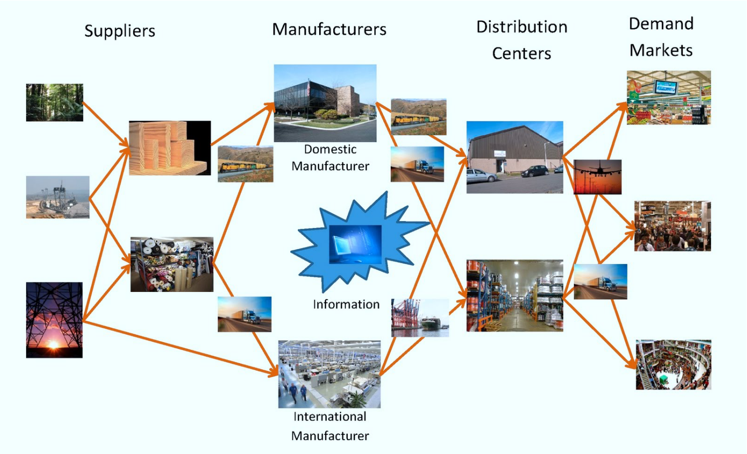
ASUS users fall victim to supply chain attack through backdoored update

Attackers hijack ASUS's auto-update process to deliver malware. Preventing such attacks is difficult, but vendors and their customers can do more to mitigate the risk.

By Lucian Constantin

Romania Correspondent, CSO | MARCH 26, 2019 04:11 AM PT

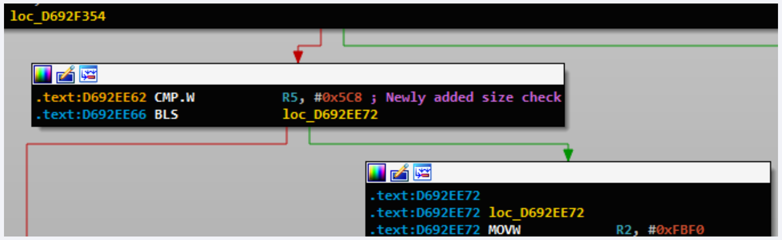
Over a million users might have downloaded and installed a backdoored version of an ASUS application that was served from the company's official update servers. The incident is the latest in a string of software supply chain attacks that have come to light over the past couple of years and highlights the need for companies to better vet the applications and updates they deploy on their systems.



The NSO WhatsApp Vulnerability – This is How It Happened

May 14, 2019

https://research.checkpoint.com/the-nso-whatsapp-vulnerability-this-is-how-it-happened/

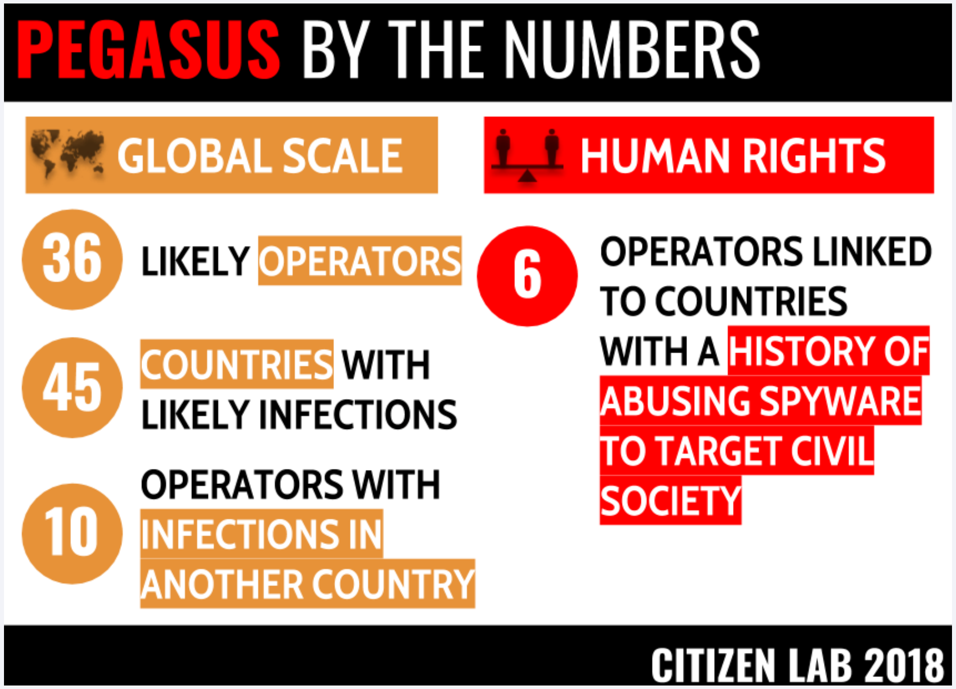


```
loc_D692F354

.text:D692EE62 CMP.W            R5, #0x5C8 ; Newly added size check
.text:D692EE66 BLS              loc_D692EE72

.text:D692EE72
.text:D692EE72 loc_D692EE72
.text:D692EE72 MOVW                 R2, #0xFBF0
```

https://www.vice.com/en_us/article/qvakb3/inside-nso-group-spyware-demo



PEGASUS BY THE NUMBERS

GLOBAL SCALE

36 LIKELY OPERATORS

45 COUNTRIES WITH LIKELY INFECTIONS

10 OPERATORS WITH INFECTIONS IN ANOTHER COUNTRY

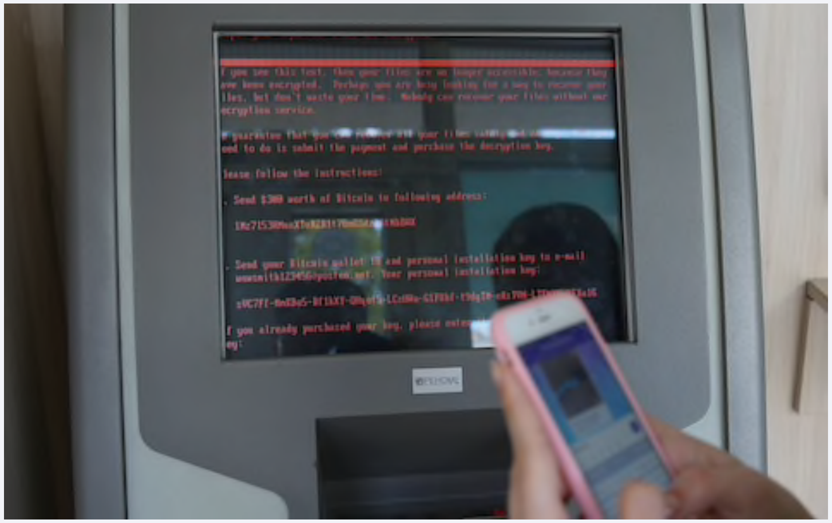
HUMAN RIGHTS

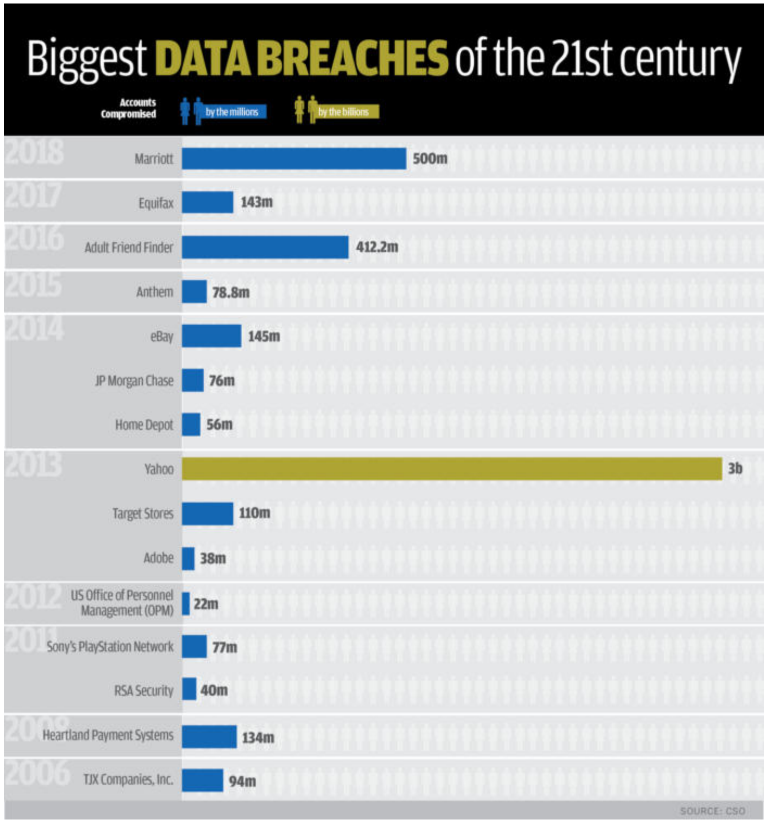
6 OPERATORS LINKED TO COUNTRIES WITH A HISTORY OF ABUSING SPYWARE TO TARGET CIVIL SOCIETY

CITIZEN LAB 2018

Emerging Cybersecurity Threats

APT





Policies and procedures

Industry standards

ITIL

COBIT

Policies and procedures

Compliance

Management

Frameworks

Best practices

and control

Framewor

Firewall

UTM

IPS

DLP

CLOUD

IAM

and control

VPN

DDoS

Protection

Device Management

IDS

Co

Antivirus

WAF

Auditing

Vulnerability Scan

Assessment

IAM

VP

IDS

Hardening

Auditing

Consulting

Training

MSS

Vulnerability

Assessment

IAM

VPN

DDoS Protection

Pentesting

IDS

Hardening

SIEM

SOA

What do we ***should target*** and what you are *really* want to **KNOW**.

Several e-assets and data on the environment, so we need to create a Cyber-Strategy considering things like:

- Industry context
- Risk
- Threat modeling
- Technologies
- Public presence
- More…

Let’s use generations...

A possible model

01 **Old School – First Gen**

A . Humans

B . Non-Centralized monitoring systems (First Gen)

02 **Current Scenario – Second Gen**

A . Log Repositories

B . SIEM

} *Add Threat Intelligence*

03 **Future – Third Gen**

A . SIEM + Steroids

B . SAO (Security Automation and Orchestration)

} *Add Artificial Intelligence*

Demo

About the Connect Platform

Catalog

Applications | Solutions | Services

from IBM, Partners, Customers

Cloud Platform

IBM Security Connect AppDev Framework

AI and analytics

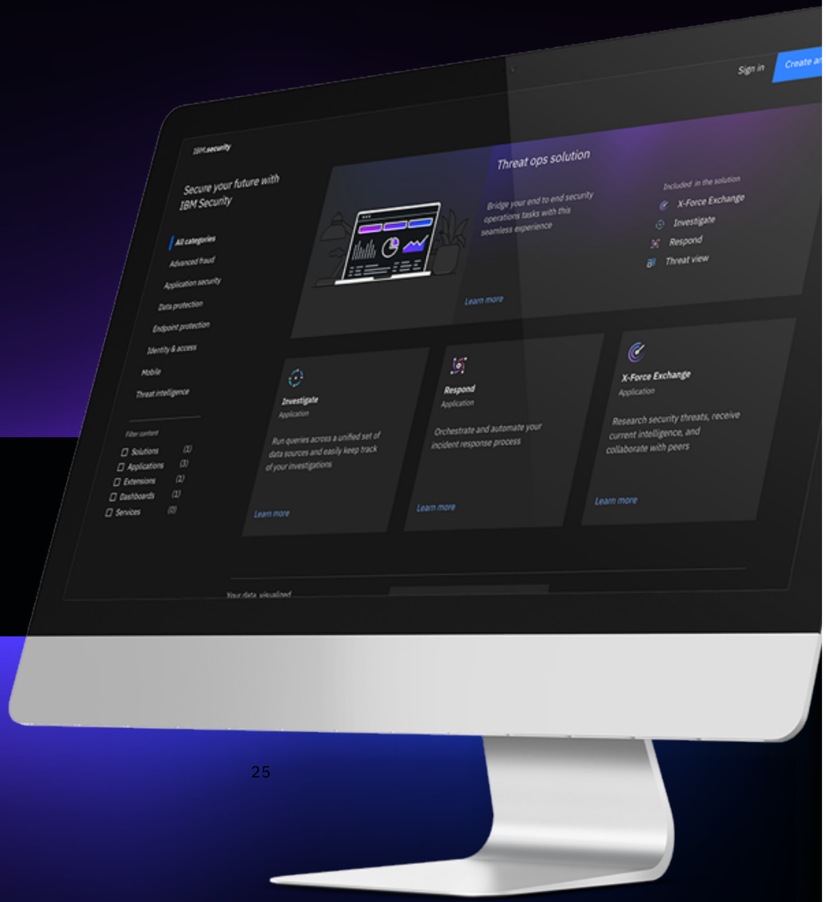
Open threat intel and data connectors

Existing infrastructure

On-premises security tools and infrastructure

Public and private clouds

Mobile devices and endpoints



Secure your future with IBM Security

Threat ops solution

Bridge your end to end security operations tasks with this seamless experience

Included in the solution

- X-Force Exchange
- Investigate
- Respond
- Threat view

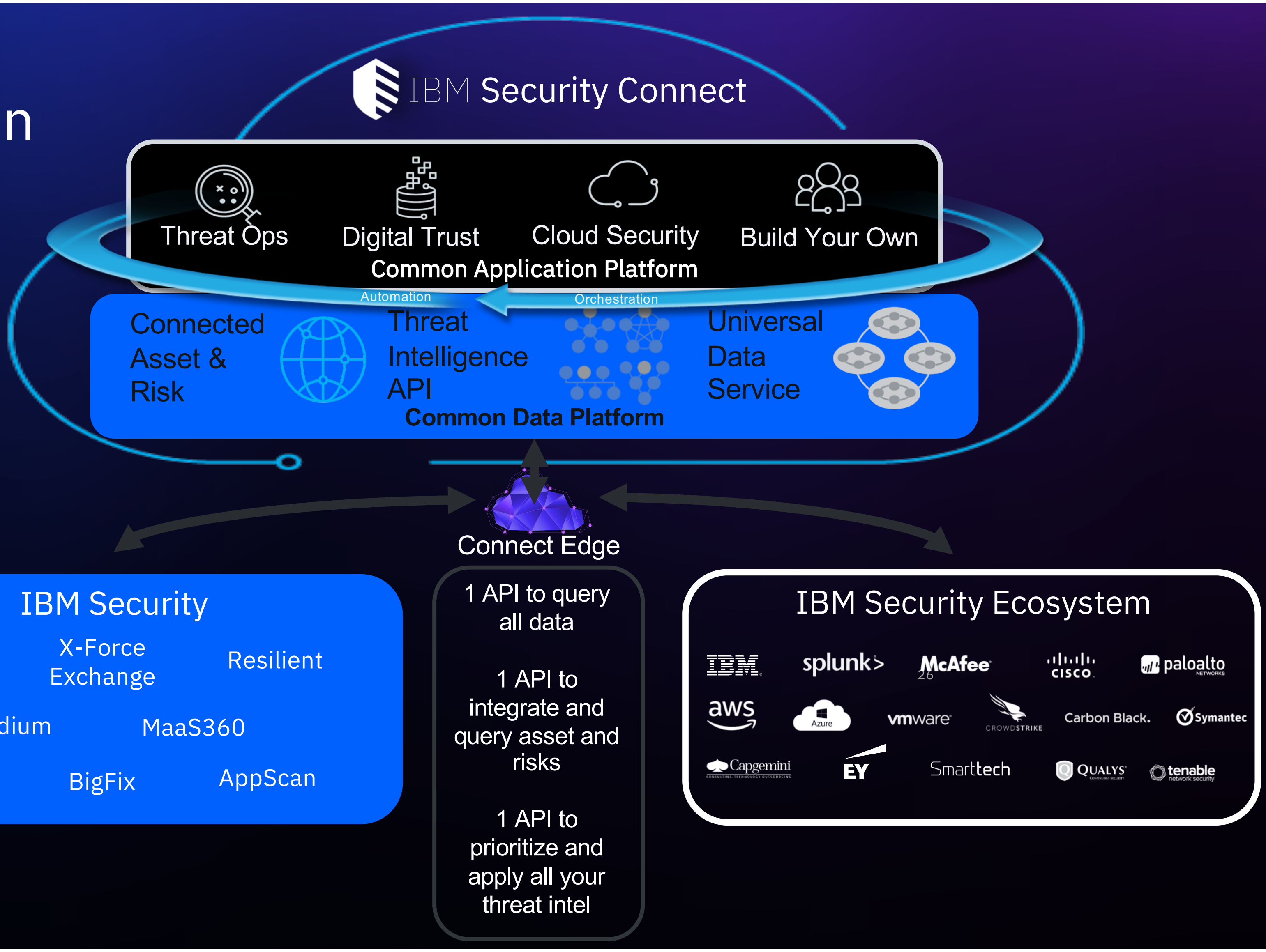
Investigate
Application
Run queries across a unified set of data sources and easily keep track of your investigations

Respond
Application
Orchestrate and automate your incident response process

X-Force Exchange
Application
Research security threats, receive current intelligence, and collaborate with peers

Your data visualized

A total integration hub for the security industry



IBM Security Connect

Threat Ops

Digital Trust

Cloud Security

Build Your Own

Common Application Platform

Automation

Orchestration

Connected Asset & Risk

Threat Intelligence API

Universal Data Service

Common Data Platform

Connect Edge

1 API to query all data

1 API to integrate and query asset and risks

1 API to prioritize and apply all your threat intel

IBM Security

QRadar

X-Force Exchange

Resilient

Guardium

MaaS360

Trusteer

BigFix

AppScan

IBM Security Ecosystem

IBM, splunk>, McAfee, cisco, paloalto networks

aws, Azure, vmware, CrowdStrike, Carbon Black., Symantec

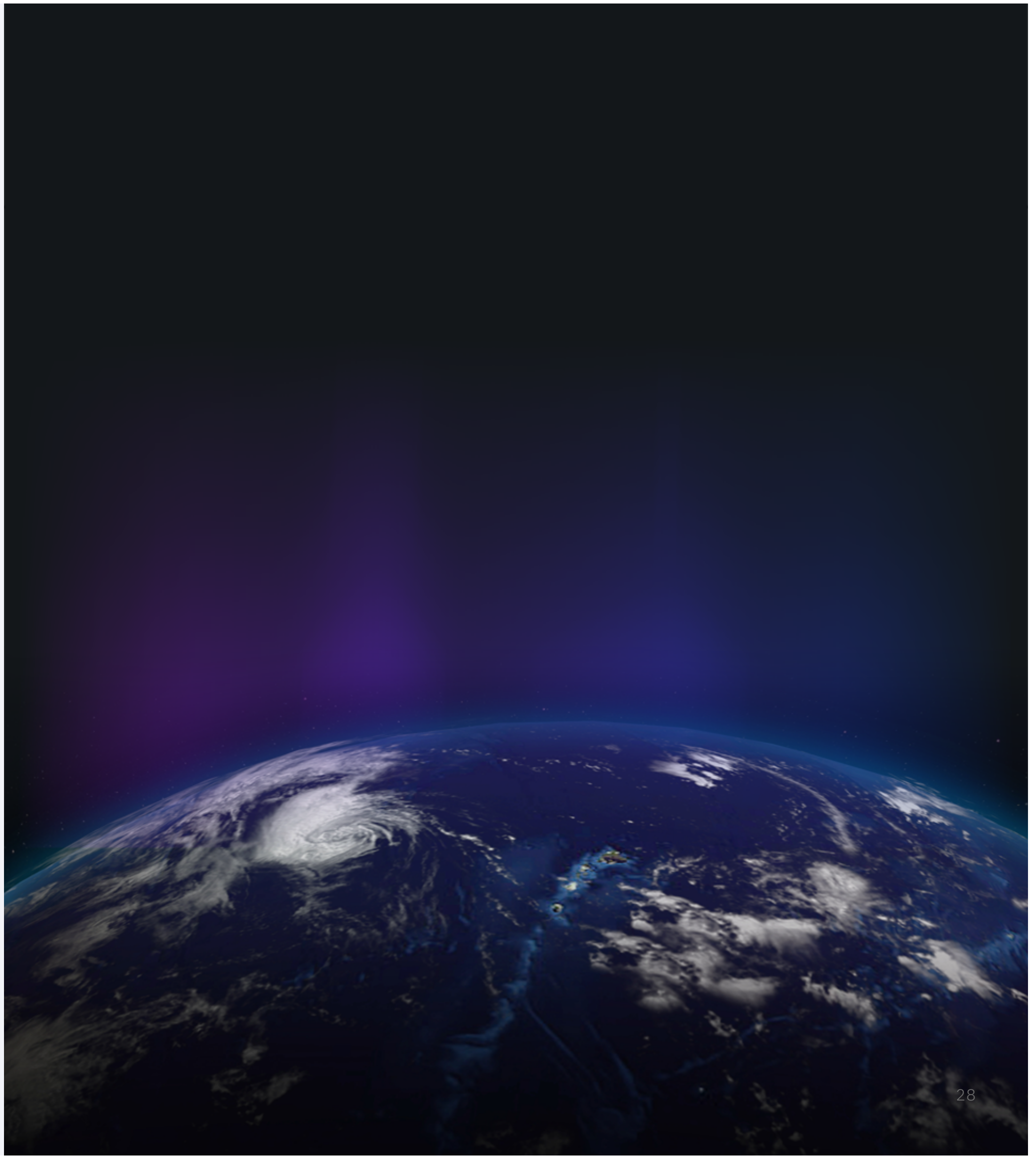
Capgemini, EY, Smarttech, Qualys, tenable network security

Where we are now

- Largest enterprise cybersecurity provider
- Leader in 12 security market segments
- 8,000+ security employees
- 20+ security acquisitions
- 70B+ security events monitored per day

LINKS

- https://exchange.xforce.ibmcloud.com
- https://app.threatconnect.com/auth/index.xhtml#/
- https://otx.alienvault.com/dashboard/new



IBM Security

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- ibm.com/security/community
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

IBM®