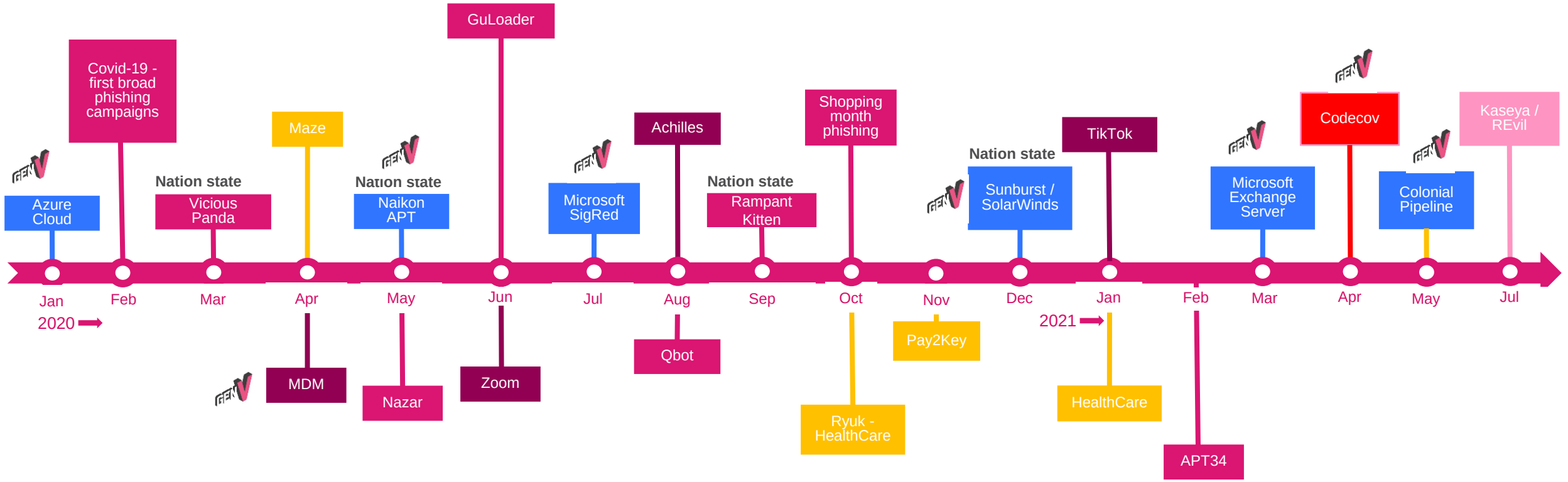
AKTUELLE BEDROHUNGSLAGE AUS SICHT VON CHECK POINT: THREAT LANDSCAPE

Armin Thommen | Manager Security Engineering, Switzerland

7.7.2022

YOU DESERVE THE BEST SECURITY

The attack surface has never been wider
2020-21 dangerous wave of cyber threats

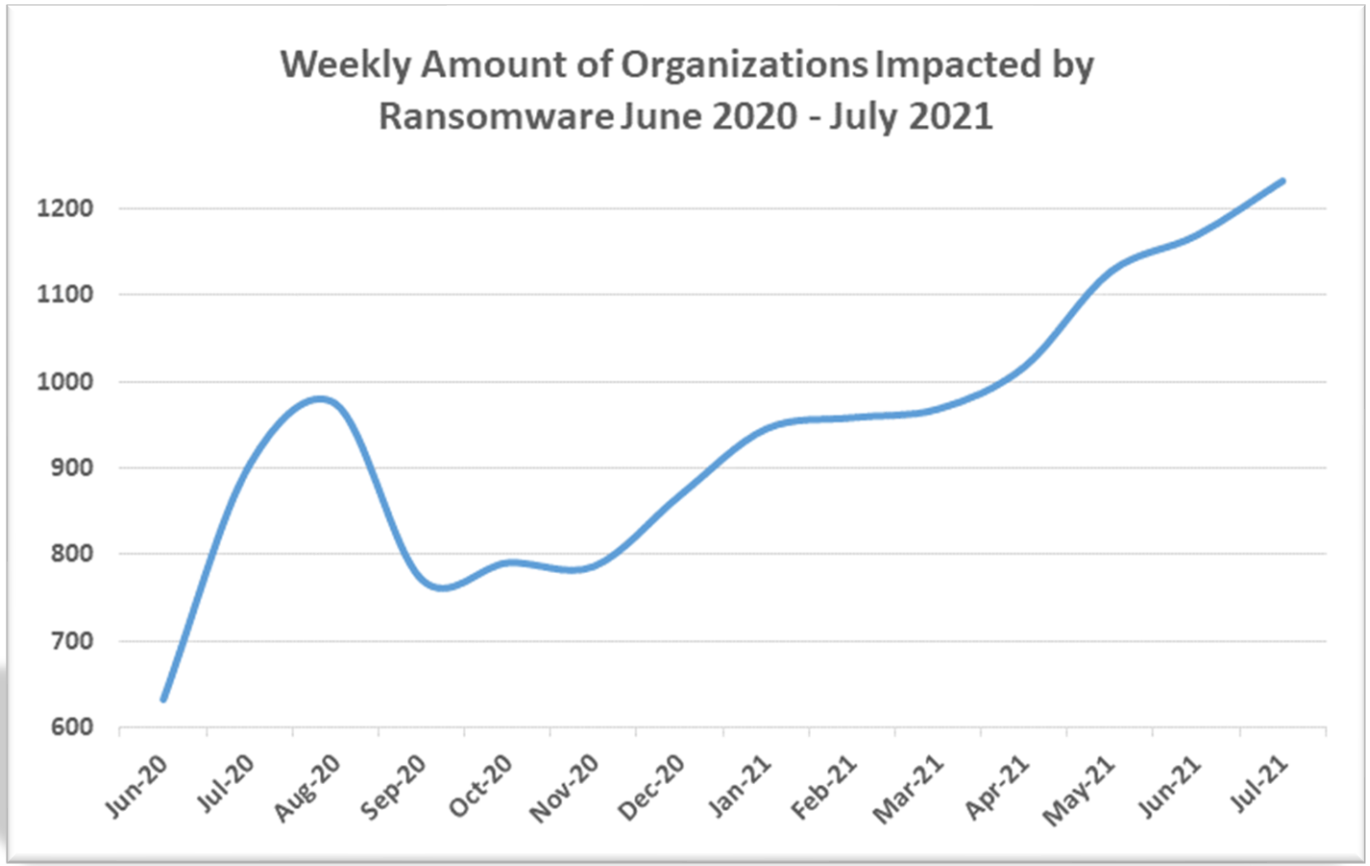


Solar winds and wild fires

Surge in Gen5 sophisticated attacks

Ransomware attacks surge globally, hitting a 93% increase year on year

- Over 1210 organizations impacted weekly
- **93% increase** year over year



Ransomware – Evolving Motivations

Financial
(Crypto currency fuels ransomware)

Data theft and Espionage
(Lazarus)

Cyber Terror and political influence
(Pay2Key)

Cyber weapon trading
(Ransomware as a service)

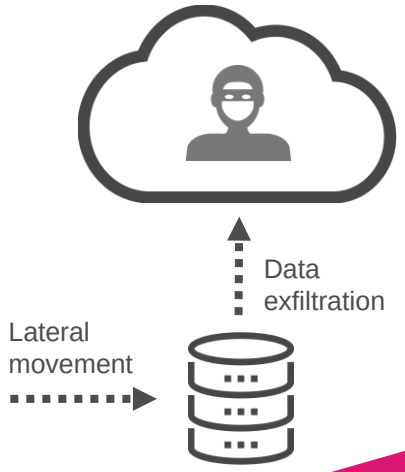
Ransomware - Evolving Tactics

Classic

"Your files are locked"

Double Extortion

"If you don't pay, we will publish your private information"



Triple Extortion

"We stole your data from the vendor you've been using"

WannaCry

2013 — $300 — **Individuals**

2017

2019 — $15M — **Companies**

2021 — $40M — **Countries**

Colonial Pipeline Company halted all the pipeline's operations

Colonial Pipeline attack - what do we know?

- **Motivation**: Financial/Target critical infrastructure
- Billing system was compromised resulting in the inability to bill the customers
- Shut down the pipeline as a precaution
- Double extortion - The attackers stole 100GB of data. threatened to release it if ransom was not paid
- Ransom paid close to $5M

Insights – Ransomware As A Service

FBI confirmed this was a DarkSide Operation

- Develop and market ransomware hacking tools
- Sells tools to “partners” to carry out attacks
- Focuses on R&D, partners on delivery
- Collecting data later to be sold and negotiated
- One of the partners claimed responsibility for carrying out the attack

Costa Rica is at War

The Guardian

Costa Rica declares national emergency amid ransomware attacks

President Rodrigo Chaves establishes emergency commission as one of his first acts amid attacks by Russian-speaking gang

THE VERGE

Costa Rican president says country is 'at war' with Conti ransomware group

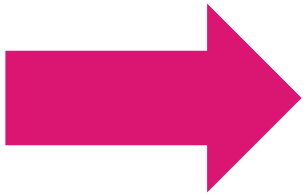
The cyberattack has disabled government systems for almost a month

By Corin Faife | @corintxt | May 18, 2022, 6:01pm EDT

What happened?

Ransomware attack against at least 27 governmental institutions:

- Ministry of Finance
- Ministry of Labor
- Ministry of Science, Technology and Telecommunications
- Ministry of Social Security
- National Meteorological Institute

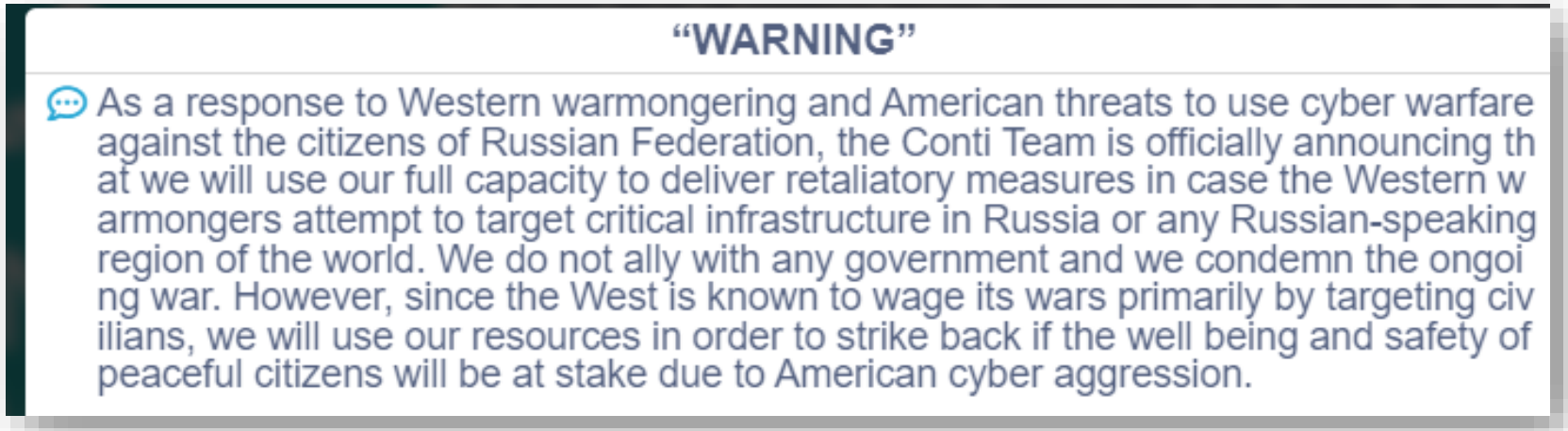


- Ministry of Finance digital services are not functioning
- Customs stopped processing import and export taxes
- Tax collection systems were paralyzed
- Salary payments to public sector employees were suspended

Conti Group

- Eastern European Ransomware Group
- More than 800 corporate victims :
  - Ireland Health Service
  - 16 U.S. Healthcare and First Responder Networks in the US
  - Cities in the US
  - Bank of Indonesia
- Connection to Ryuk, Trickbot, Emotet
- Revenue – at least $180M in 2021
- Double extortion – shame blog

Ukraine Russia War - Conti Group Takes Side



Greetings,

Here is a friendly heads-up that the Conti gang has just lost all their shit. Please know this is true.
https://twitter.com/ContiLeaks/status/1498030708736073734 >
https://anonfiles.com/VeP6K6K5xc/1_tgz

The link will take you to download an 1.tgz file that can be unpacked running tar -xzvf 1.tgz command in your terminal .
The contents of the first dump contain the chat communications (current, as of today and going to the past) of the Conti Ransomware gang. We promise it is very interesting.

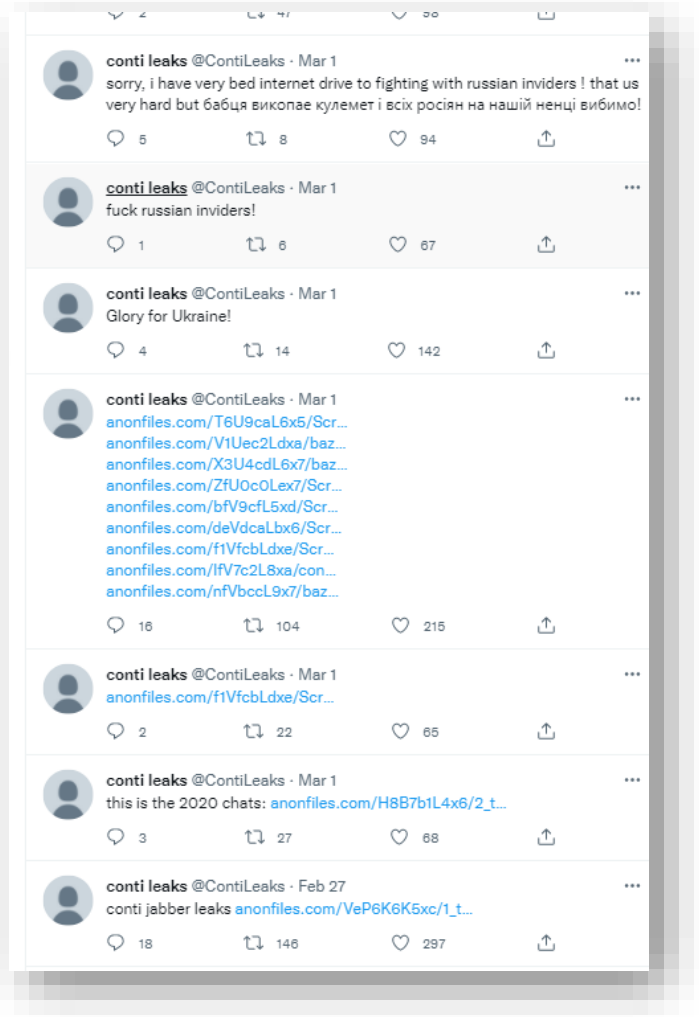
There are more dumps coming , stay tuned.
You can help the world by writing this as your top story.

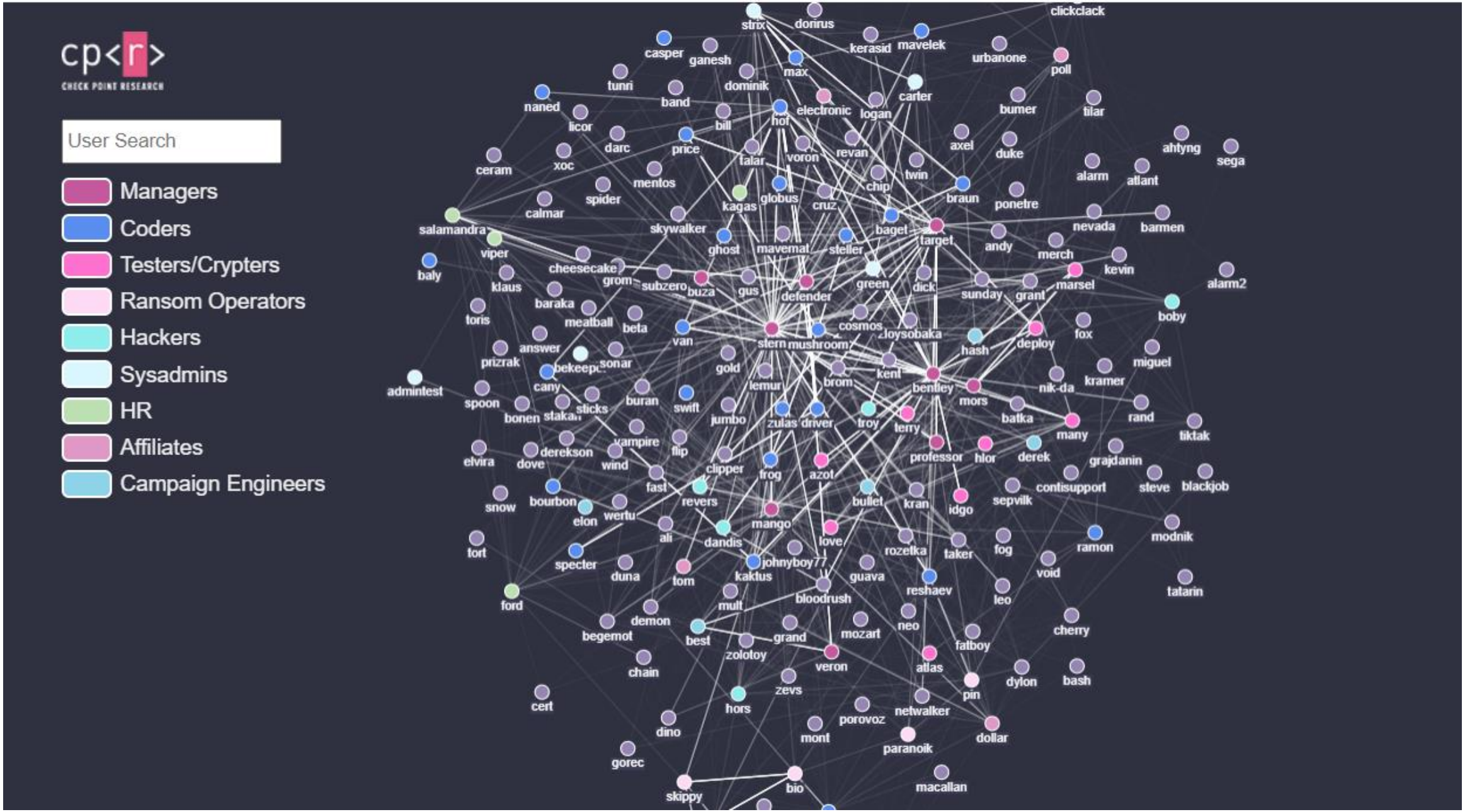
It is not malware or a joke.
This is being sent to many journalists and researchers.

Thank you for your support

Glory to Ukraine!

Ukrainian Researcher Leaks Internal Data of Conti





Group Structure – Tech Company

- Developers
- QA
- Cryptographers
- Reverse Engineers
- Pentesters
  - At least 5 separate group led by “team leads”
- HR
- DevOps/ IT
- OSINT Specialists
- Negotiators
- Offices in Russia

Employee of the month….

2021-10-29 13:10:34

Silver

share the title employee of the month @collin and @ryan

2021-10-29 13:11:02

Silver

collin for overcoming the situation with the backconnect and in general for pulling the project in such difficult conditions

2021-10-29 13:11:15

Silver

ryan for taking the initiative with the new delivery method

2021-10-29 13:11:30

angelo

:partying_face:

2021-10-29 13:11:31

Silver

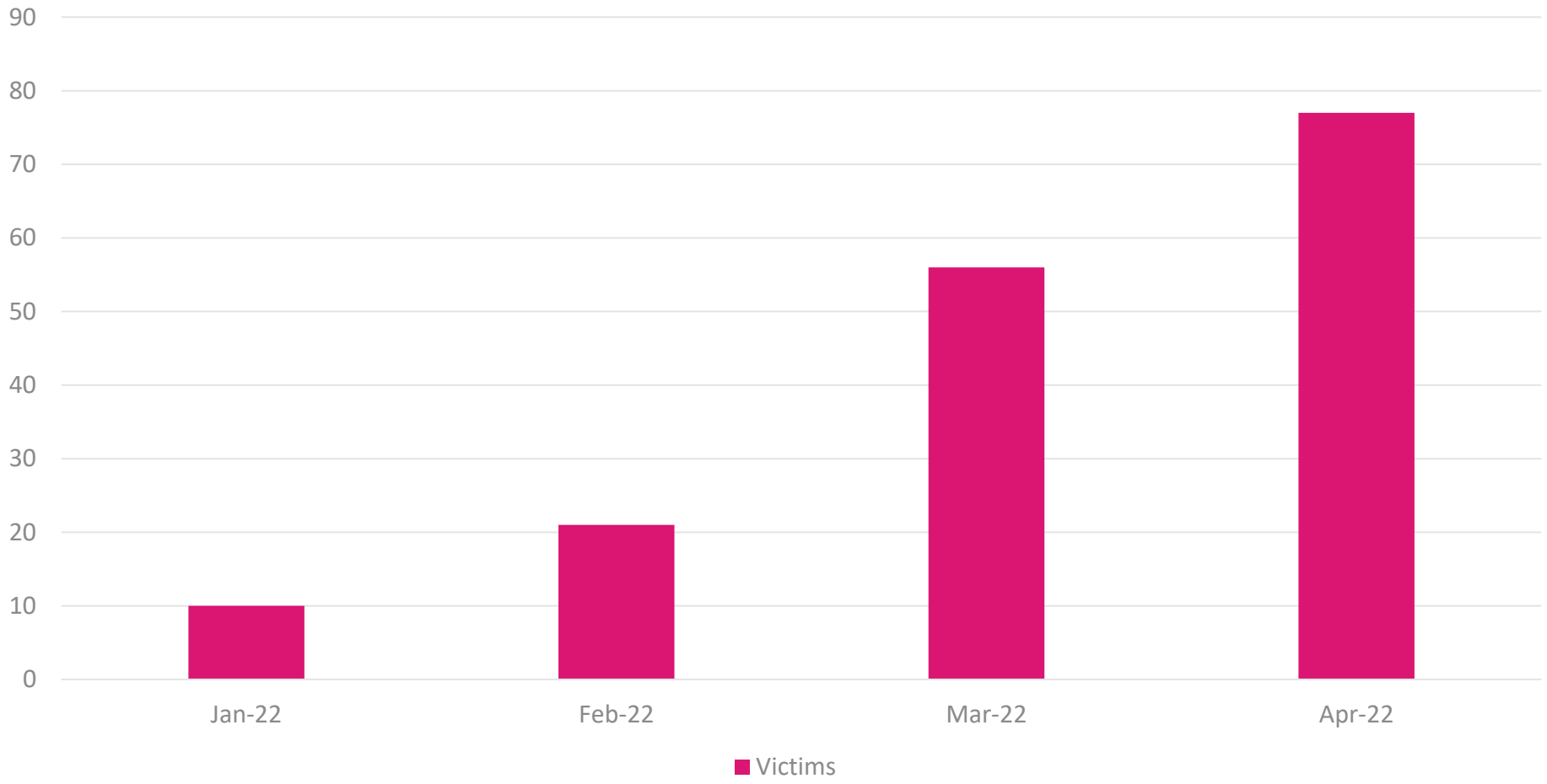
both bonuses of $500

- Commission models
- Employee referral program
- Performance reviews

Leaks of Conti Ransomware Group Paint Picture of a Surprisingly Normal Tech Start-Up... Sort Of

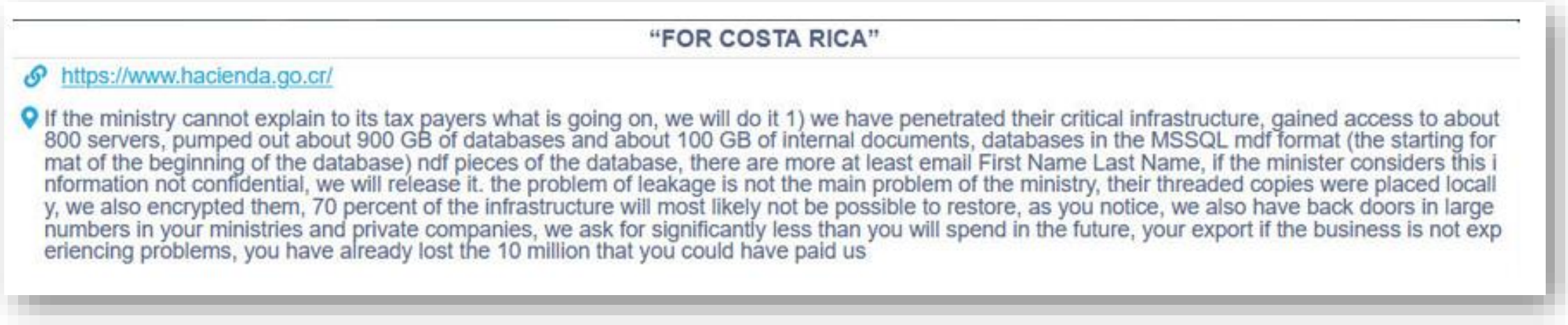
March 10, 2022

Conti Victims 2022 – Growing Aggressiveness



April 17th - Seemingly Regular Post Appeared

April 20 – More Aggressive Tone towards Costa Rica



"FOR COSTA RICA"

https://www.hacienda.go.cr/

If the ministry cannot explain to its tax payers what is going on, we will do it 1) we have penetrated their critical infrastructure, gained access to about 800 servers, pumped out about 900 GB of databases and about 100 GB of internal documents, databases in the MSSQL mdf format (the starting for mat of the beginning of the database) ndf pieces of the database, there are more at least email First Name Last Name, if the minister considers this i nformation not confidential, we will release it. the problem of leakage is not the main problem of the ministry, their threaded copies were placed locall y, we also encrypted them, 70 percent of the infrastructure will most likely not be possible to restore, as you notice, we also have back doors in large numbers in your ministries and private companies, we ask for significantly less than you will spend in the future, your export if the business is not exp eriencing problems, you have already lost the 10 million that you could have paid us

"The problem of the leakage is not the biggest problem of the ministry…we have also backdoors in large numbers in you ministries and private companies … "

May 6 – US State Department Offers a Reward for Conti Leaders

$10,000,000

Week of May 8 – New Sworn President Declares State of Emergency

- May 8th – Inauguration of President Rodrigo Chaves
- May 11th – Declaration on state of emergency

Artículo 1

Versión del artículo: 1 de 1

Nº 43542-MP-MICITT
EL PRESIDENTE DE LA REPÚBLICA,
LA MINISTRA DE LA PRESIDENCIA
Y EL MINISTRO DE CIENCIA INNOVACIÓN TECNOLOGÍA Y TELECOMUNICACIONES

En ejercicio de las facultades que les confieren los artículos 140 incisos 3), 6), 16), 18), 146 y 180 de la Constitución Política; artículos 25 inciso 1), 27 inciso 1), 28 inciso 2) subíndice b), de la Ley General de la Administración Pública, Ley número 6227 del 2 de mayo de 1978; el artículo 29 de la Ley Nacional de Emergencias y Prevención del Riesgo.

CONSIDERANDO:

I. Que el artículo 140 de la Constitución Política, establece que son deberes y atribuciones del Presidente y del respectivo Ministro de Gobierno, vigilar el buen funcionamiento de los servicios y dependencias administrativas.

II. Que la Ley General de la Administración Pública, Ley Nº 6227, del 2 de mayo de 1978, establece en su artículo 4, que la actividad de los entes públicos deberá estar sujeta en su conjunto a los principios fundamentales del servicio público, para asegurar su continuidad, su eficiencia, su adaptación a todo cambio en el régimen legal o en la necesidad social que satisfacen y la igualdad en el trato de los destinatarios, usuarios o beneficiarios.

III. Que la misma Ley General de la Administración Pública, establece en el artículo 12, que se considerará autorizado un servicio público cuando se haya indicado el sujeto y el fin del mismo.

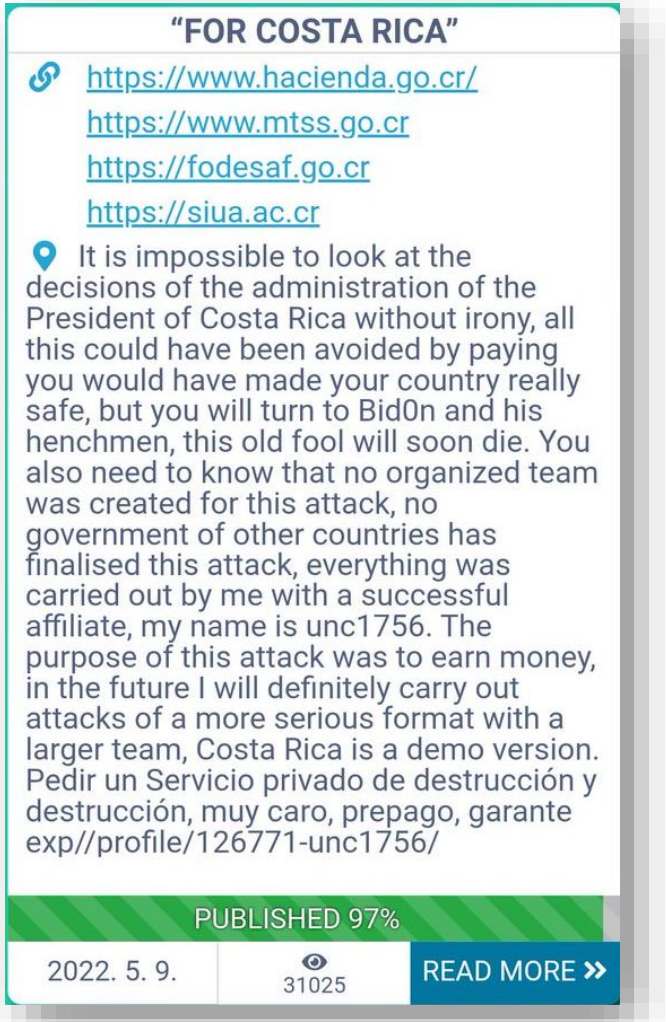
IV. Que la Ley Nacional de Emergencias y Prevención del Riesgo, Ley Nº8488 del 22 de noviembre de 2006, establece en el artículo primero que regulará las acciones ordinarias, establecidas en su artículo 14, las cuales el Estado Costarricense deberá desarrollar para reducir las causas de las pérdidas de vidas y las consecuencias sociales, económicas y ambientales, inducidas por los factores de riesgo de origen natural y antrópico; así como la actividad extraordinaria que el Estado deberá efectuar en caso de estado de emergencia, para lo cual se aplicará un régimen de excepción. Así mismo, el numeral 29 establece que en caso de calamidad pública ocasionada por hechos de la naturaleza o del ser humano, que son imprevisibles o previsibles pero inevitables y no pueden ser controlados por las potestades ordinarias que dispone la Administración Pública; el Poder Ejecutivo está facultado para declarar emergencia nacional a fin de integrar y definir las responsabilidades y funciones de todos los organismos, entidades públicas, privadas, a efectos de poder brindar una solución acorde a la magnitud del situación de calamidad.

V. Que el artículo 4 de la Ley N º 8488 de cita define que el Estado de Emergencia debe ser decretado *"(. . .) con fundamento en un estado de necesidad y urgencia, ocasionado* ***por circunstancias de guerra, conmoción interna y calamidad pública.*** *Esta declaratoria permite gestionar, por la vía de excepción, las acciones y la asignación de los recursos necesarios para atender la emergencia, de conformidad con el artículo 180 de la Constitución Política"*, así como que, la emergencia en sí es un *"Estado de crisis provocado por el desastre y basado en la magnitud de los daños y las pérdidas. Es un estado de necesidad y urgencia que obliga a tomar acciones inmediatas con el fin de* ***salvar vidas y bienes, evitar el sufrimiento y atender las necesidades de los afectados.*** *Puede ser manejada en tres fases progresivas: respuesta, rehabilitación y reconstrucción; se extiende en el tiempo hasta que se logre controlar definitivamente la situación"* y por desastre, que es una *"Situación o proceso que se desencadena como resultado de un fenómeno de origen natural,* ***tecnológico o provocado por el hombre que,*** *al encontrar, en una población, condiciones propicias de vulnerabilidad,* ***causa alteraciones intensas en las condiciones normales de funcionamiento de la comunidad, tales como pérdida de vidas y de salud de la población, destrucción o pérdida de bienes de la colectividad*** *y daños severos al ambiente".*

Conti's Quick Reaction

"It is impossible to look in the decisions of President of Costa Rica without irony.. But you would turn to Bid0n and his henchmen, this old fool will soon die"

"In the future I will definitely carry out attacks of a more serious format with a larger team, Costa Rica is a demo version"

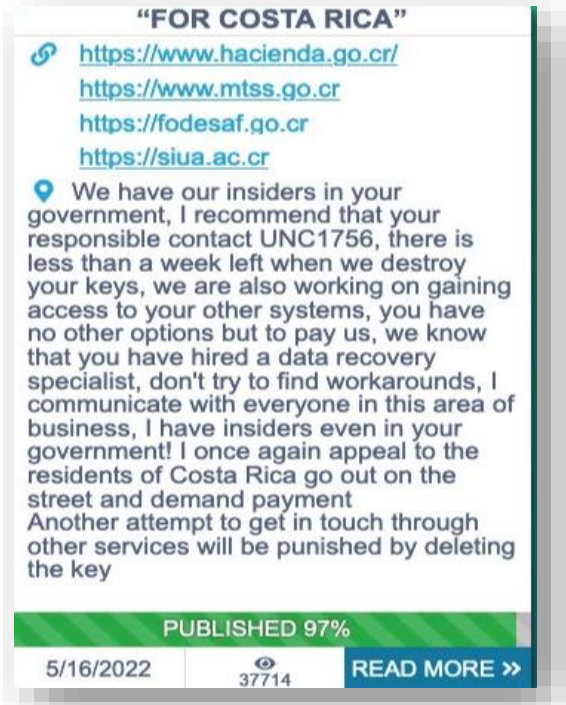


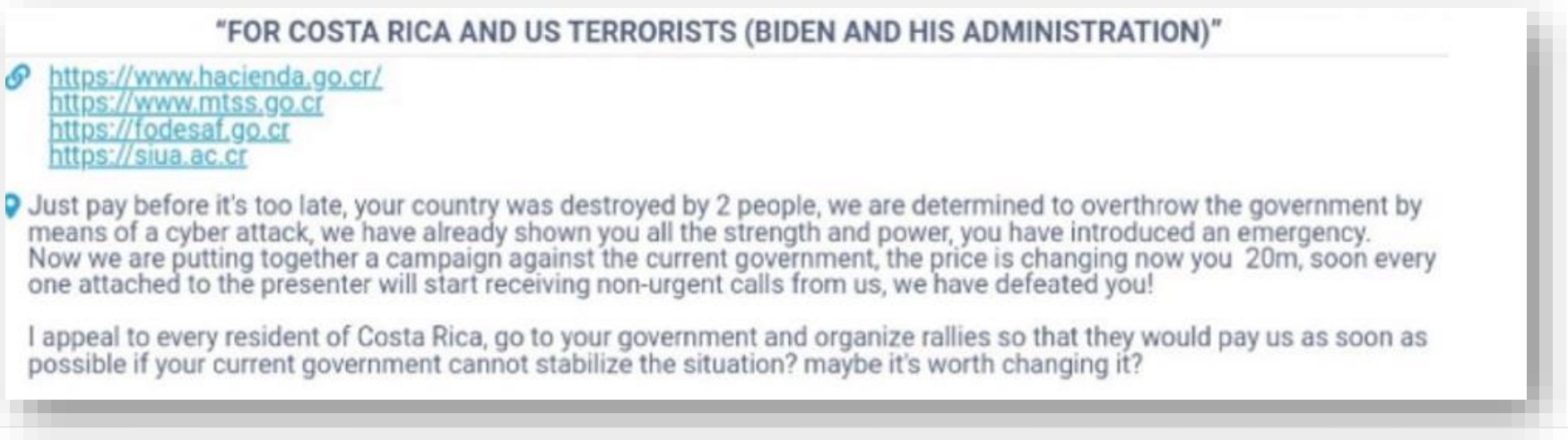
Week of May 14th – Triple Extortion and Riot Calls

“We have our insiders in your government”

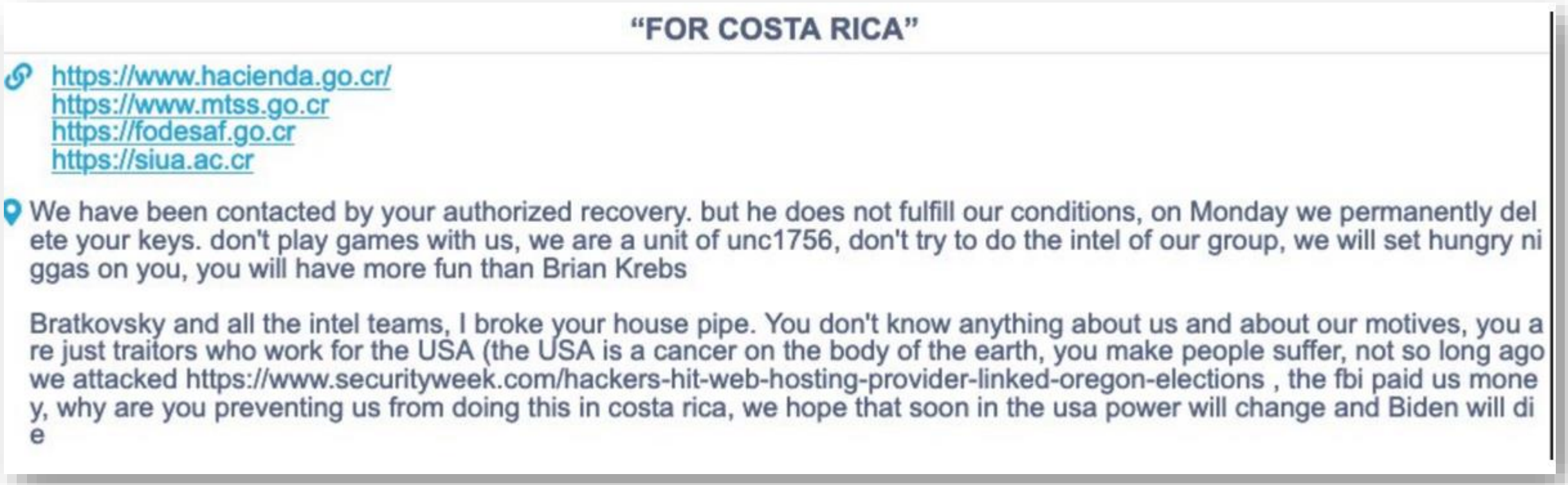
“Your country will be destroyed by just 2 people, we are determined to overthrow the government by means of cyber attack.. Now we are putting together a campaign against the current government…”

“I appeal to every citizen of Costa Rica… go and organize rallies. Maybe it worth changing the government…”



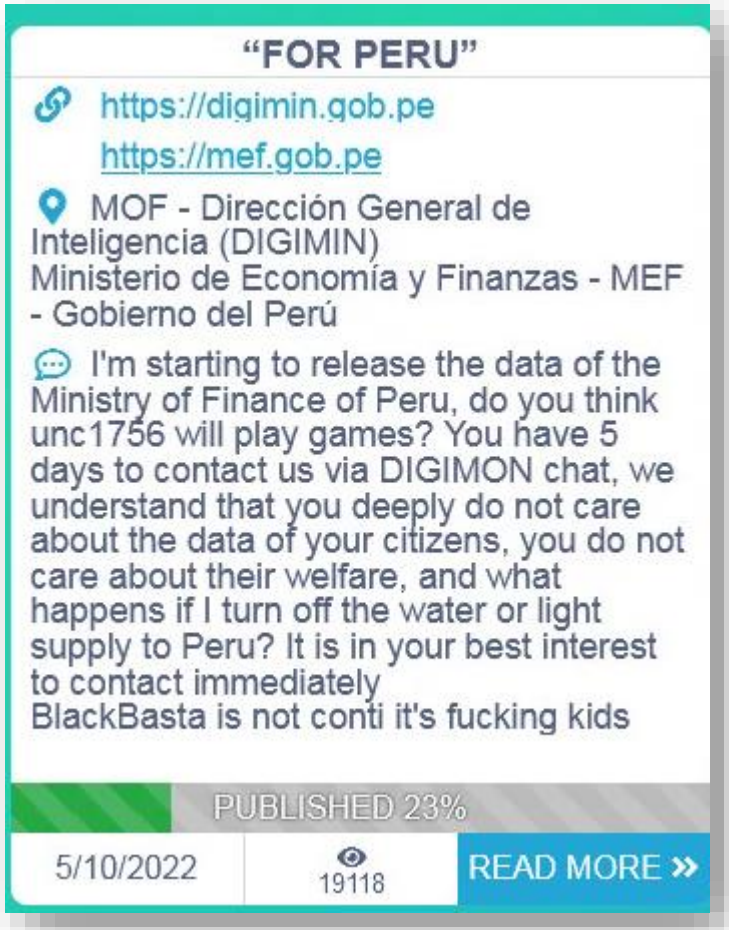


May 20th – Previously Unseen Rhetoric Against US



"You are just traitors who work for the US – the US is a cancer in the body of the earth, you make people suffer … the FBI paid us money.. We hope the USA power will change and Biden will die."

In Parallel – Country Extortion of Peru



The End?

BLEEPINGCOMPUTER

Conti ransomware finally shuts down data leak, negotiation sites

By Lawrence Abrams

June 24, 2022 10:35 AM 2

TC

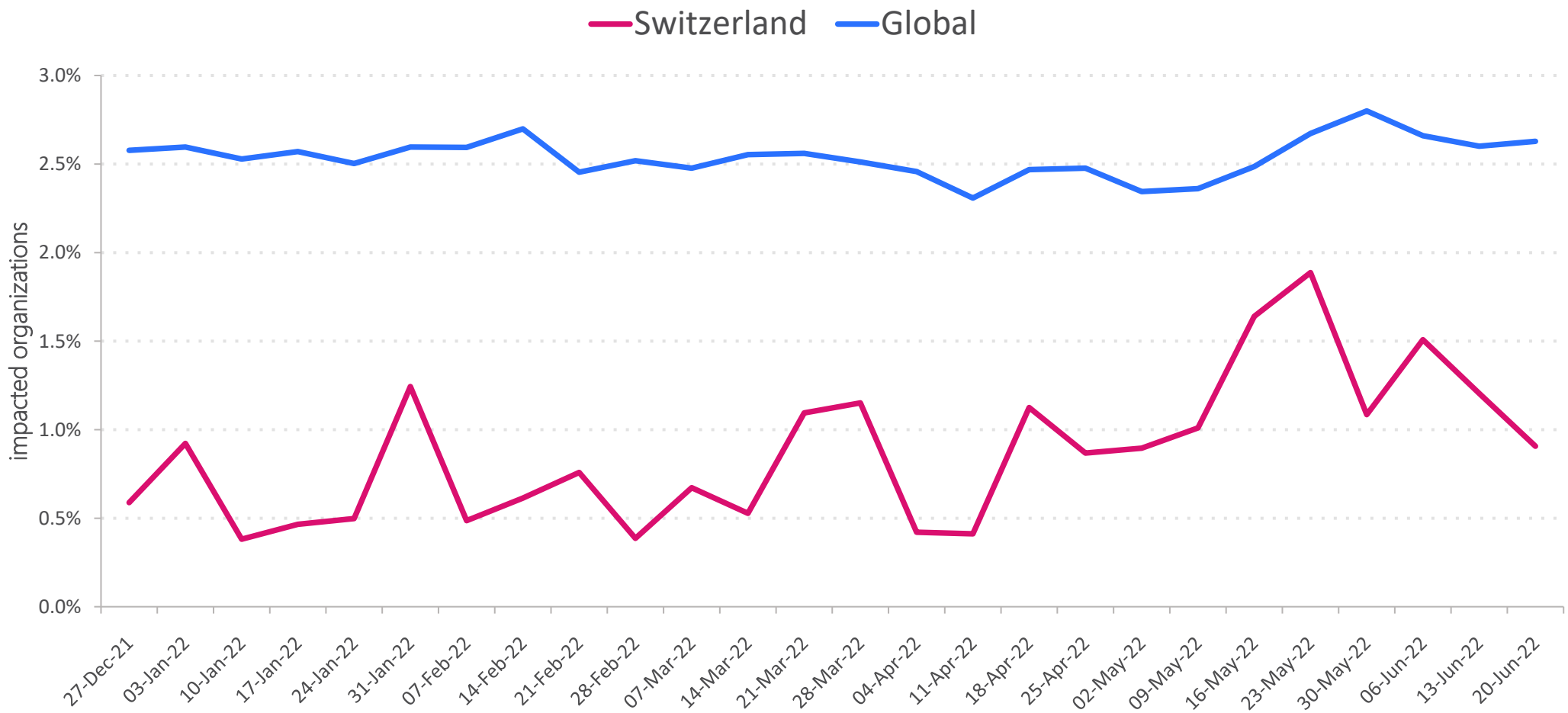
Costa Rica's public health system hit by Hive ransomware following Conti attacks

Carly Page @carlypage_ / 5:59 PM GMT+3 • June 1, 2022 Comment

Future Implications – the B2G Model

- Large, organized groups > more professional
- Going after the big money
- Country extortion affecting
  - International geopolitics
  - Internal politics

Ransomware Attacks- Last 6 Months



How to protect pre and post?

- Data back up
- Recovery plan
- Update/patch systems regularly
- Invest in cyber security awareness and training for employees

- Network segmentation
- Use multi-factor authentication
- Use anti-ransomware and threat prevention tools
- Disable hyperlinks in received emails

Don’t wait till it’s too late. Protect your organization from the next Ransomware Attack

Step Up to Gen 5 of Cyber Security with Check Point

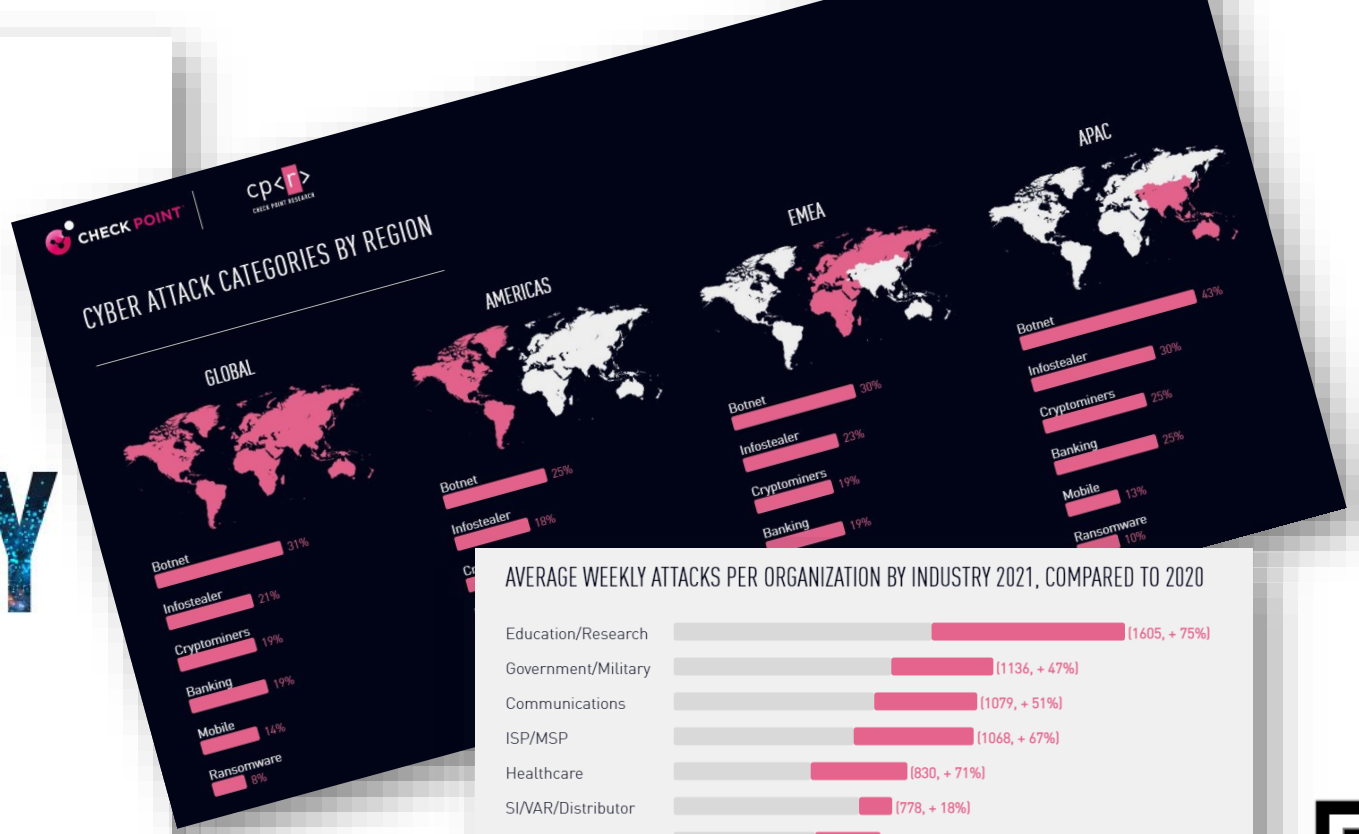
- **Deploy Anti-Ransomware** solution on all your end-point devices
- **Prevent malicious attachments** from reaching your corporate emails
- **Prevent users from downloading malware & Zero-Days** from the internet and private emails
- **Inspect traffic**, files and updates used by your internet facing applications
- **Block infected machines** from communicating with C&C
- Exercise and implement **Incident response** to call in the case of emergency

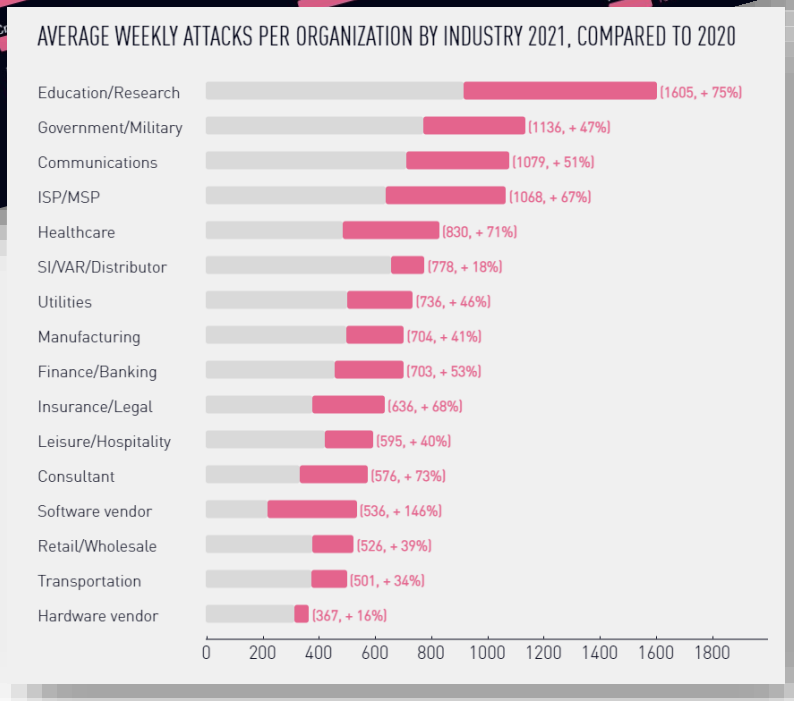
CHECK POINT

CYBER SECURITY REPORT

2022

cp<r>
CHECK POINT RESEARCH





https://go.checkpoint.com/security-report/

THANK YOU

YOU DESERVE THE BEST SECURITY