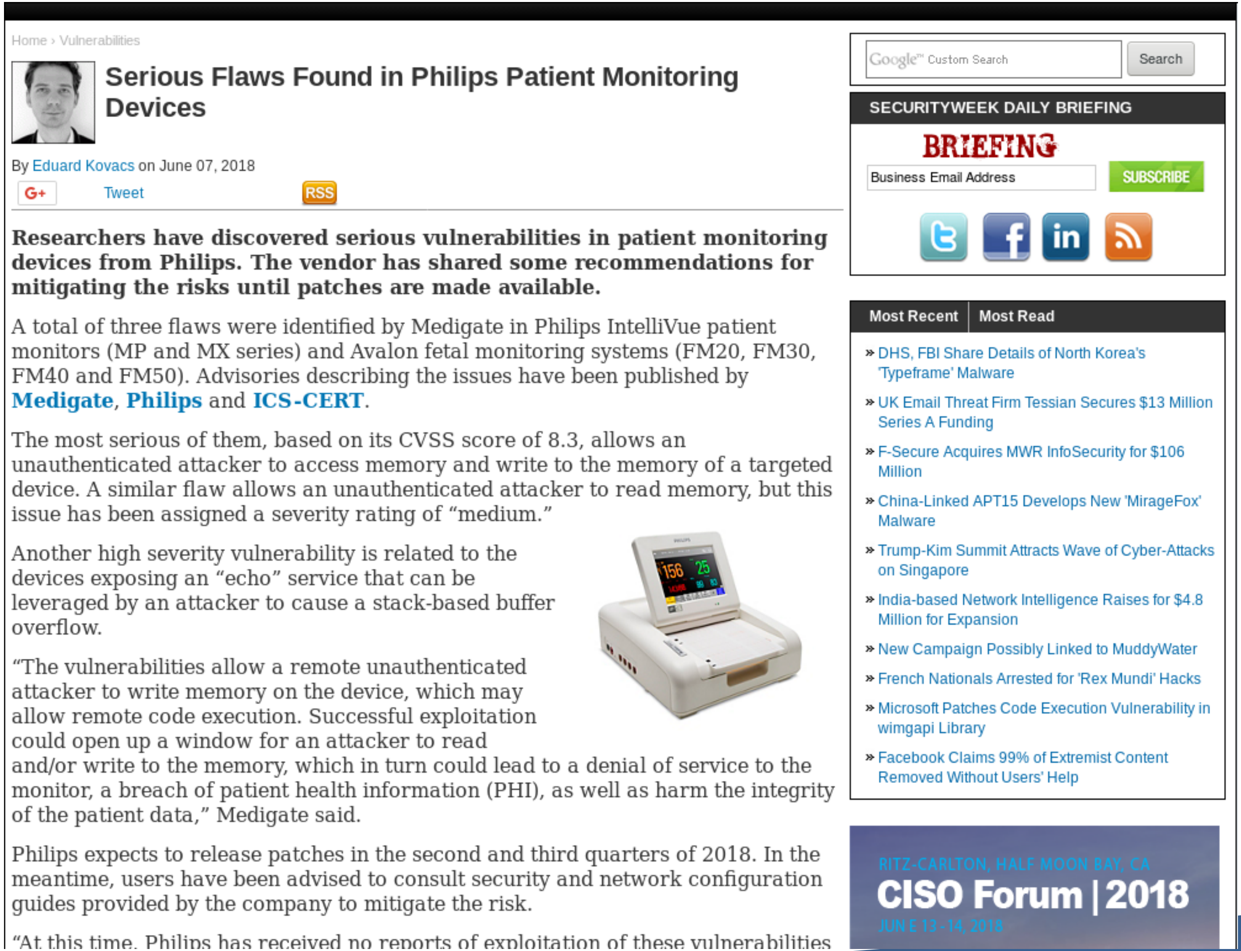
Ciberamenazas
Sector Salud

SIN CLASIFICAR



Serious Flaws Found in Philips Patient Monitoring Devices

By Eduard Kovacs on June 07, 2018

Researchers have discovered serious vulnerabilities in patient monitoring devices from Philips. The vendor has shared some recommendations for mitigating the risks until patches are made available.

A total of three flaws were identified by Medigate in Philips IntelliVue patient monitors (MP and MX series) and Avalon fetal monitoring systems (FM20, FM30, FM40 and FM50). Advisories describing the issues have been published by **Medigate**, **Philips** and **ICS-CERT**.

The most serious of them, based on its CVSS score of 8.3, allows an unauthenticated attacker to access memory and write to the memory of a targeted device. A similar flaw allows an unauthenticated attacker to read memory, but this issue has been assigned a severity rating of “medium.”

Another high severity vulnerability is related to the devices exposing an “echo” service that can be leveraged by an attacker to cause a stack-based buffer overflow.

“The vulnerabilities allow a remote unauthenticated attacker to write memory on the device, which may allow remote code execution. Successful exploitation could open up a window for an attacker to read and/or write to the memory, which in turn could lead to a denial of service to the monitor, a breach of patient health information (PHI), as well as harm the integrity of the patient data,” Medigate said.

Philips expects to release patches in the second and third quarters of 2018. In the meantime, users have been advised to consult security and network configuration guides provided by the company to mitigate the risk.

“At this time, Philips has received no reports of exploitation of these vulnerabilities

SECURITYWEEK DAILY BRIEFING

BRIEFING

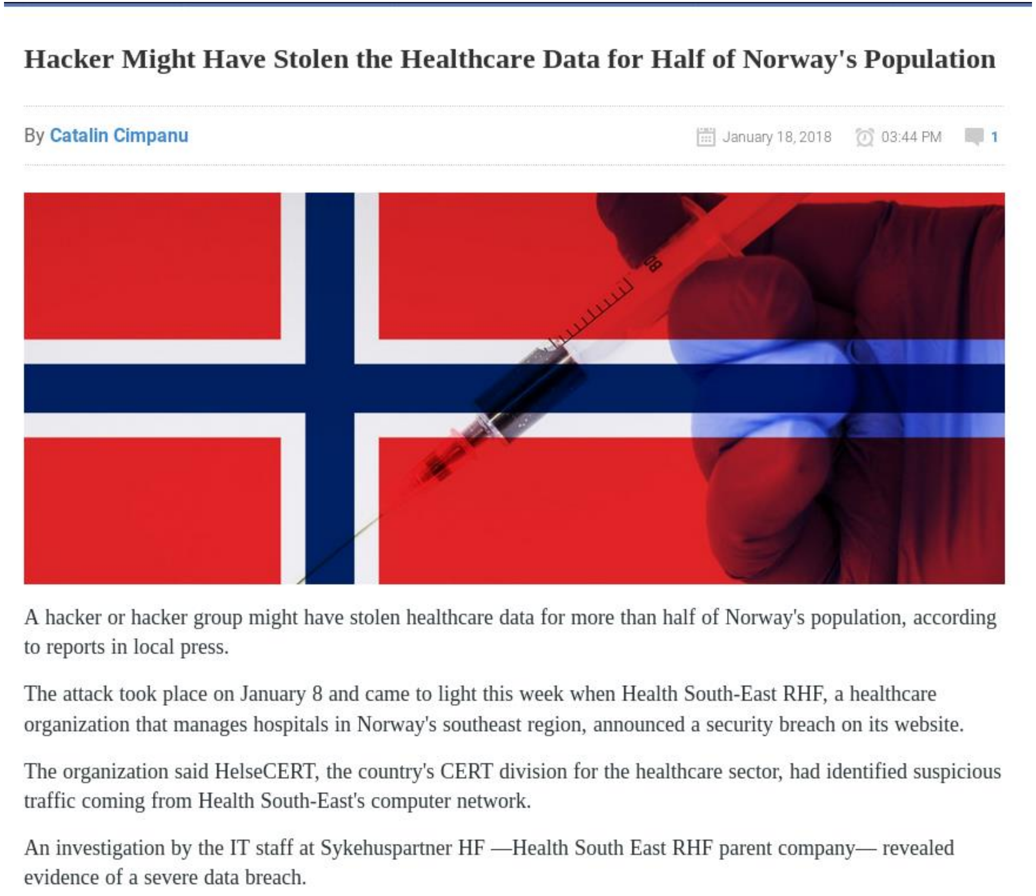
Business Email Address

SUBSCRIBE

Most Recent | Most Read

- » DHS, FBI Share Details of North Korea's 'Typeframe' Malware
- » UK Email Threat Firm Tessian Secures $13 Million Series A Funding
- » F-Secure Acquires MWR InfoSecurity for $106 Million
- » China-Linked APT15 Develops New 'MirageFox' Malware
- » Trump-Kim Summit Attracts Wave of Cyber-Attacks on Singapore
- » India-based Network Intelligence Raises for $4.8 Million for Expansion
- » New Campaign Possibly Linked to MuddyWater
- » French Nationals Arrested for 'Rex Mundi' Hacks
- » Microsoft Patches Code Execution Vulnerability in wimgapi Library
- » Facebook Claims 99% of Extremist Content Removed Without Users' Help

RITZ-CARLTON, HALF MOON BAY, CA
CISO Forum | 2018
JUNE 13 - 14, 2018



Hacker Might Have Stolen the Healthcare Data for Half of Norway's Population

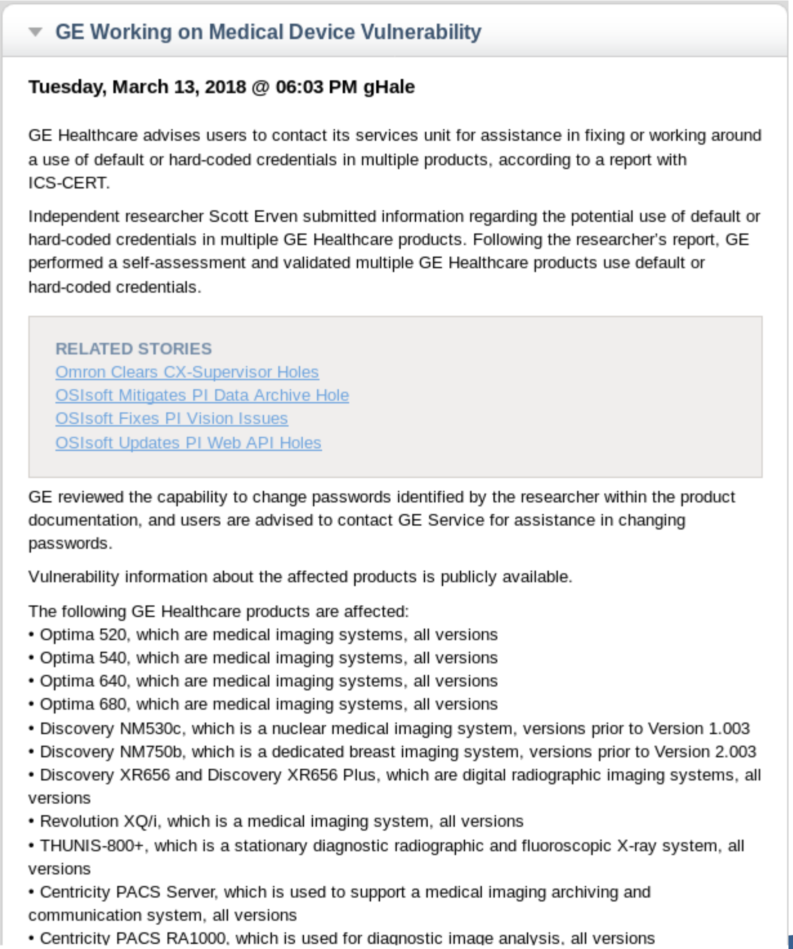
By **Catalin Cimpanu** January 18, 2018 03:44 PM 1

A hacker or hacker group might have stolen healthcare data for more than half of Norway's population, according to reports in local press.

The attack took place on January 8 and came to light this week when Health South-East RHF, a healthcare organization that manages hospitals in Norway's southeast region, announced a security breach on its website.

The organization said HelseCERT, the country's CERT division for the healthcare sector, had identified suspicious traffic coming from Health South-East's computer network.

An investigation by the IT staff at Sykehuspartner HF —Health South East RHF parent company— revealed evidence of a severe data breach.



GE Working on Medical Device Vulnerability

Tuesday, March 13, 2018 @ 06:03 PM gHale

GE Healthcare advises users to contact its services unit for assistance in fixing or working around a use of default or hard-coded credentials in multiple products, according to a report with ICS-CERT.

Independent researcher Scott Erven submitted information regarding the potential use of default or hard-coded credentials in multiple GE Healthcare products. Following the researcher's report, GE performed a self-assessment and validated multiple GE Healthcare products use default or hard-coded credentials.

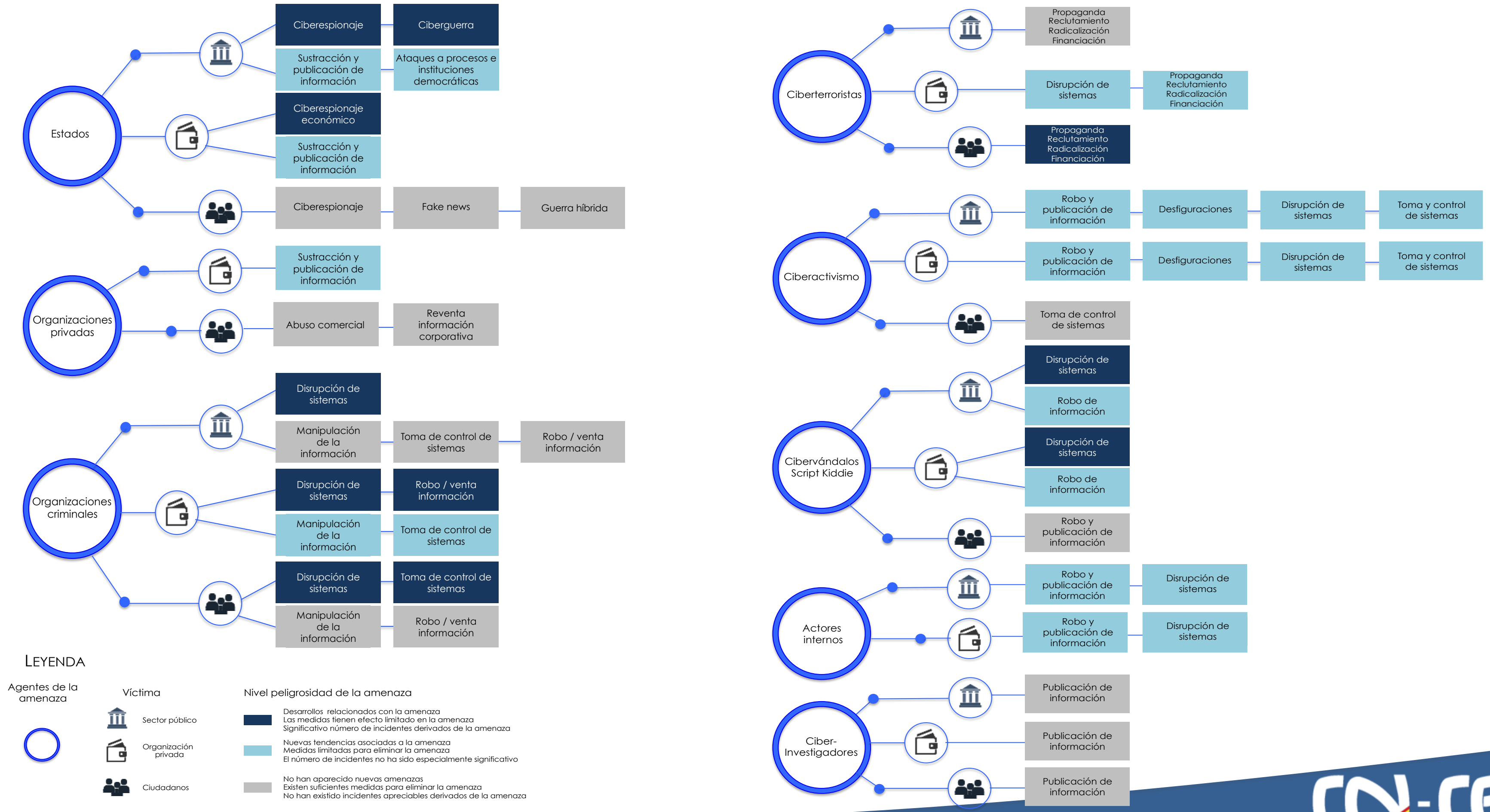
RELATED STORIES
Omron Clears CX-Supervisor Holes
OSIsoft Mitigates PI Data Archive Hole
OSIsoft Fixes PI Vision Issues
OSIsoft Updates PI Web API Holes

GE reviewed the capability to change passwords identified by the researcher within the product documentation, and users are advised to contact GE Service for assistance in changing passwords.

Vulnerability information about the affected products is publicly available.

The following GE Healthcare products are affected:
- Optima 520, which are medical imaging systems, all versions
- Optima 540, which are medical imaging systems, all versions
- Optima 640, which are medical imaging systems, all versions
- Optima 680, which are medical imaging systems, all versions
- Discovery NM530c, which is a nuclear medical imaging system, versions prior to Version 1.003
- Discovery NM750b, which is a dedicated breast imaging system, versions prior to Version 2.003
- Discovery XR656 and Discovery XR656 Plus, which are digital radiographic imaging systems, all versions
- Revolution XQ/i, which is a medical imaging system, all versions
- THUNIS-800+, which is a stationary diagnostic radiographic and fluoroscopic X-ray system, all versions
- Centricity PACS Server, which is used to support a medical imaging archiving and communication system, all versions
- Centricity PACS RA1000, which is used for diagnostic image analysis, all versions

Ciberseguridad en el Sector Salud



Estados
- 🏛
  - ■ Ciberespionaje
  - ■ Ciberguerra
  - ▨ Sustracción y publicación de información
  - ▨ Ataques a procesos e instituciones democráticas
- 👛
  - ■ Ciberespionaje económico
  - ▨ Sustracción y publicación de información
- 👥
  - □ Ciberespionaje
  - □ Fake news
  - □ Guerra híbrida

Organizaciones privadas
- 👛
  - ▨ Sustracción y publicación de información
- 👥
  - □ Abuso comercial
  - □ Reventa información corporativa

Organizaciones criminales
- 🏛
  - ■ Disrupción de sistemas
  - □ Manipulación de la información
  - □ Toma de control de sistemas
  - □ Robo / venta información
- 👛
  - ■ Disrupción de sistemas
  - ■ Robo / venta información
  - ▨ Manipulación de la información
  - ▨ Toma de control de sistemas
- 👥
  - ■ Disrupción de sistemas
  - ■ Toma de control de sistemas
  - □ Manipulación de la información
  - □ Robo / venta información

Ciberterroristas
- 🏛
  - □ Propaganda Reclutamiento Radicalización Financiación
- 👛
  - ▨ Disrupción de sistemas
  - ▨ Propaganda Reclutamiento Radicalización Financiación
- 👥
  - ■ Propaganda Reclutamiento Radicalización Financiación

Ciberactivismo
- 🏛
  - ▨ Robo y publicación de información
  - ▨ Desfiguraciones
  - ▨ Disrupción de sistemas
  - ▨ Toma y control de sistemas
- 👛
  - ▨ Robo y publicación de información
  - ▨ Desfiguraciones
  - ▨ Disrupción de sistemas
  - ▨ Toma y control de sistemas
- 👥
  - □ Toma de control de sistemas

Cibervándalos Script Kiddie
- 🏛
  - ■ Disrupción de sistemas
  - ▨ Robo de información
- 👛
  - ■ Disrupción de sistemas
  - ▨ Robo de información
- 👥
  - □ Robo y publicación de información

Actores internos
- 🏛
  - ▨ Robo y publicación de información
  - ▨ Disrupción de sistemas
- 👛
  - ▨ Robo y publicación de información
  - ▨ Disrupción de sistemas

Ciber-Investigadores
- 🏛
  - □ Publicación de información
- 👛
  - □ Publicación de información
- 👥
  - □ Publicación de información

LEYENDA

Agentes de la amenaza ○

Víctima
- 🏛 Sector público
- 👛 Organización privada
- 👥 Ciudadanos

Nivel peligrosidad de la amenaza
- ■ Desarrollos relacionados con la amenaza
  Las medidas tienen efecto limitado en la amenaza
  Significativo número de incidentes derivados de la amenaza
- ▨ Nuevas tendencias asociadas a la amenaza
  Medidas limitadas para eliminar la amenaza
  El número de incidentes no ha sido especialmente significativo
- □ No han aparecido nuevas amenazas
  Existen suficientes medidas para eliminar la amenaza
  No han existido incidentes apreciables derivados de la amenaza

Fuente: Cyber Security Assessment Netherlands. CSAN 2017 y elaboración propia

HERRAMIENTAS DE LA CIBERGUERRA

- Diplomacia y acciones de inteligencia tradicional
- Actos subversivos y de sabotaje
- Influencia política y económica
- Instrumentalización del crimen organizado
- Operaciones psicológicas
- Propaganda y desinformación
- Ciberataques

RESUMEN 2017

Demostración fuerza

Wannacry 2.0
(mayo 2017)

OwnCloud
(febrero 2017)

Sabotaje

LexNet
(julio 2017)

Saguaro
(enero 2017)

Struts
(marzo 2017)

APACHE STRUTS2
REMOTE
-> CODE
-> EXECUTE
VULNERABILITY
(CVE-2017-5638, S2-045)

notPetya
(junio 2017)

#OpCatalunya
(oct. 2017)

OpCatalunya
Phase 2
Follow

Nama Tikure
@NamaTikure

No! We will not stop the attacks against Spain. #OpCatalunya Phase 2 #FreeCatalonia.

New attacks is coming. #Anonymous

4:18 PM - Oct 23, 2017

110 863 1,402

2017

Emissary Panda
(febrero 2017)

APT28
(julio 2017)

Emissary Panda
(julio 2017)

Snake
(julio 2017)

Hidden Cobra
(nov. 2017)

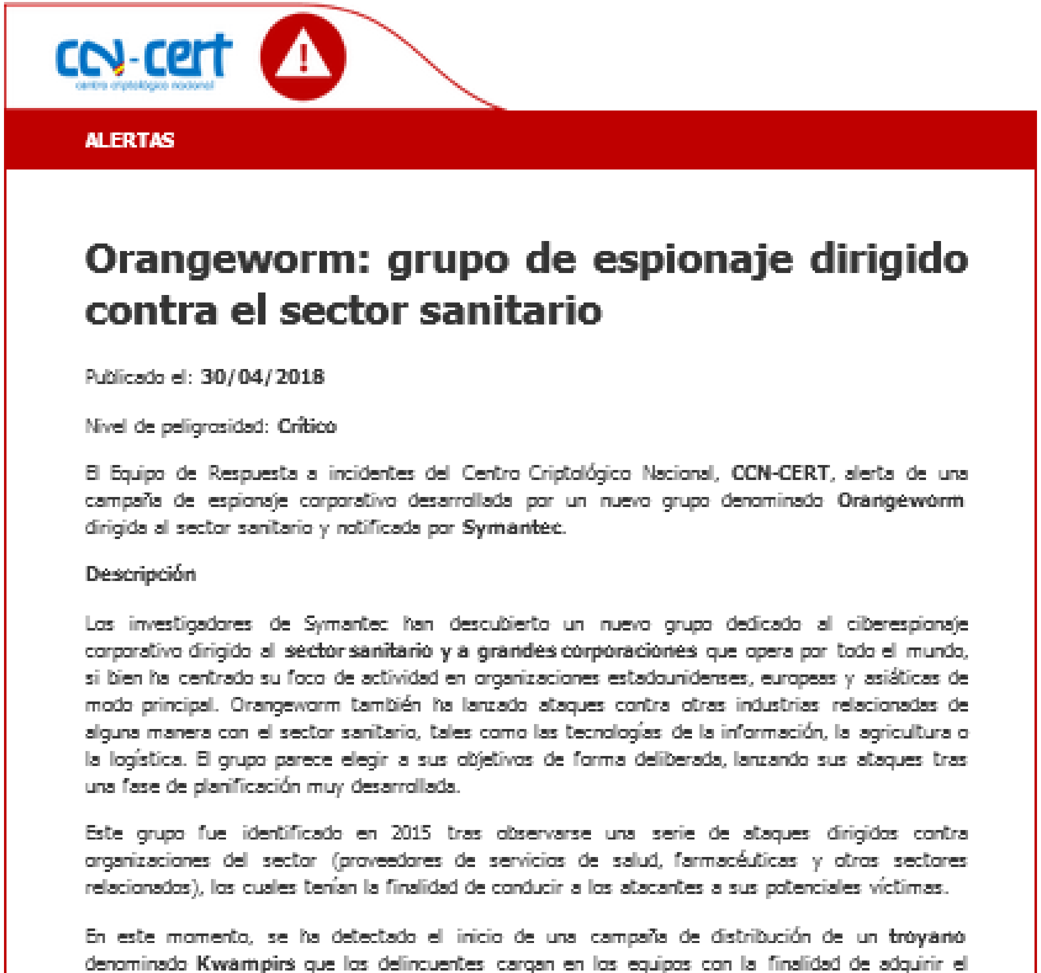
APT10
(abril 2017)

Snake
(sep. 2017)

Grizzly Steppe
(enero 2017)

Espionaje

Desinformación Elecciones USA



Orangeworm: grupo de espionaje dirigido contra el sector sanitario

Publicado el: **30/04/2018**

Nivel de peligrosidad: **Crítico**

El Equipo de Respuesta a incidentes del Centro Criptológico Nacional, **CCN-CERT**, alerta de una campaña de espionaje corporativo desarrollada por un nuevo grupo denominado **Orangeworm** dirigida al sector sanitario y notificada por **Symantec**.

Descripción

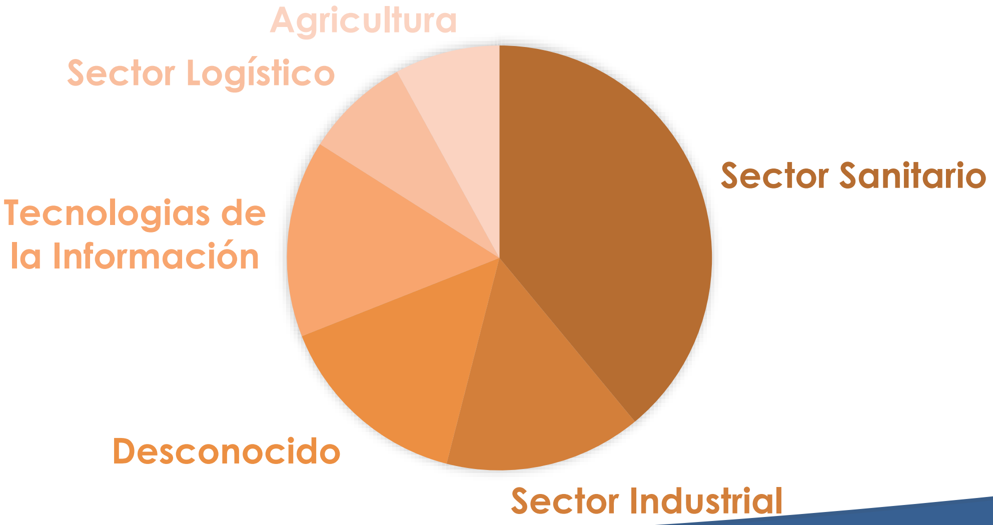
Los investigadores de Symantec han descubierto un nuevo grupo dedicado al ciberespionaje corporativo dirigido al **sector sanitario y a grandes corporaciones** que opera por todo el mundo, si bien ha centrado su foco de actividad en organizaciones estadounidenses, europeas y asiáticas de modo principal. Orangeworm también ha lanzado ataques contra otras industrias relacionadas de alguna manera con el sector sanitario, tales como las tecnologías de la información, la agricultura o la logística. El grupo parece elegir a sus objetivos de forma deliberada, lanzando sus ataques tras una fase de planificación muy desarrollada.

Este grupo fue identificado en 2015 tras observarse una serie de ataques dirigidos contra organizaciones del sector (proveedores de servicios de salud, farmacéuticas y otros sectores relacionados), los cuales tenían la finalidad de conducir a los atacantes a sus potenciales víctimas.

En este momento, se ha detectado el inicio de una campaña de distribución de un **troyano** denominado **Kwampirs** que los delincuentes cargan en los equipos con la finalidad de adquirir el

Orangeworm (abril 2018)

- Operando desde el año 2015 (EEUU, Europa y Asia).
- Objetivo: grandes empresas internacionales y organizaciones de salud con el fin de realizar espionaje corporativo.
- También ataques contra otras empresas y sectores proveedores del sector salud.



Orangeworm (abril 2018)

- No eligen a sus víctimas al azar. Seleccionan los objetivos deliberada y cuidadosamente, llevando a cabo una planificación concienzuda antes de lanzar el ataque.
- Carga malware en dispositivos que alojan software empleado para controlar:
  - Máquinas de rayos X
  - Resonancia Magnética Nuclear (RMN)
- También dispositivos utilizados para ayudar a los pacientes a completar los formularios de consentimiento para procedimientos médicos.

Orangeworm (abril 2018)

COMPROMISO

- Infiltración en la red y despliegue del troyano con funcionalidades de puerta trasera Trojan.Kwampirs.
- Implementa técnicas de evasión de detección por hash de la muestra.
- Se asegura la persistencia creando un servicio.
- Recoge información del equipo comprometido para ver si es de interés y si puede infectar otros equipos visibles desde este equipo.

Orangeworm (abril 2018)

RECOLECCIÓN DE INFORMACIÓN

- Los atacantes proceden a reunir toda la información posible:
  - Información de la red
  - Equipos accedidos recientemente
  - Información del adaptador de red
  - Recursos compartidos de red visibles
  - Unidades mapeadas
  - Archivos en el propio equipo

Orangeworm (abril 2018)

PROPAGACIÓN

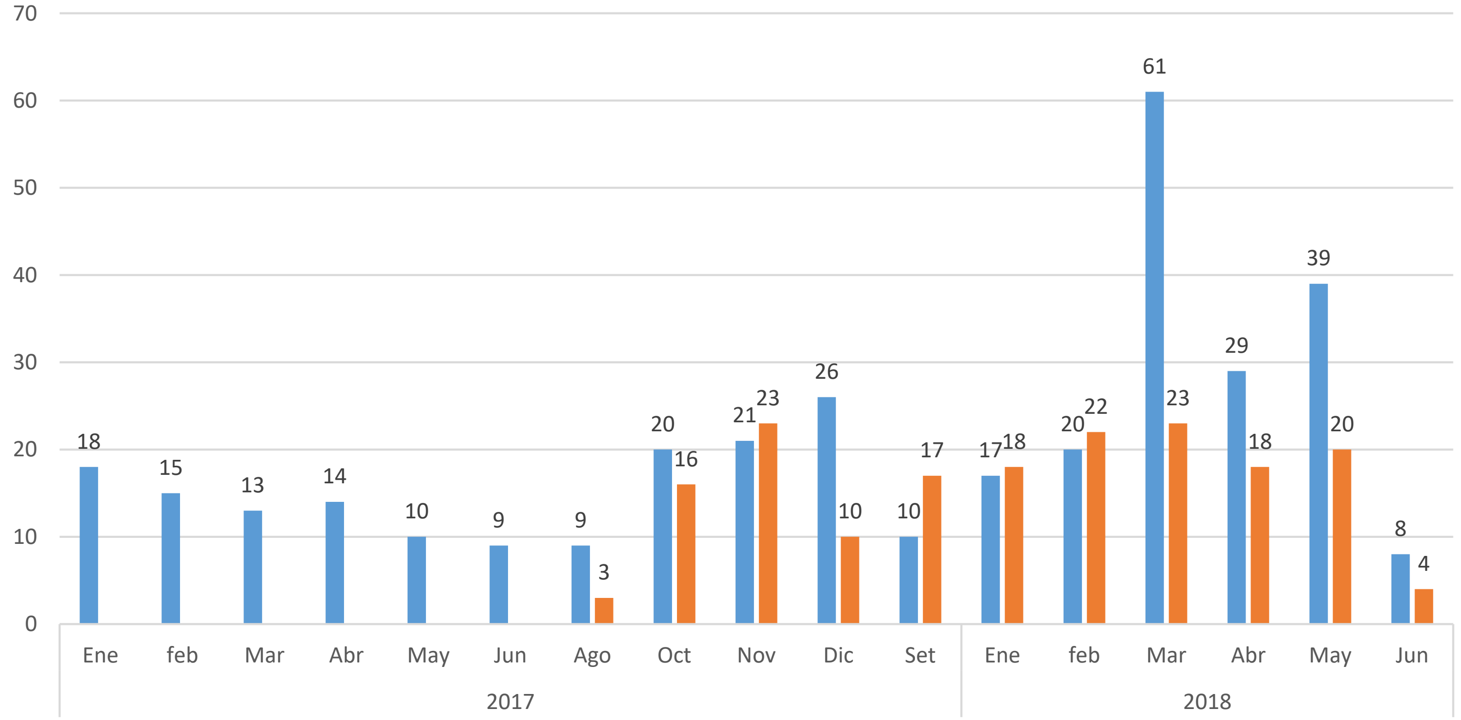
- Utilizan métodos bastante agresivos de propagación.
- Se copia a si mismo en recursos de red compartidos.
  - Procedimiento de propagación bastante antiguo
  - Funciona en entornos que utilizan sistemas operativos obsoletos como Windows XP
- Gran impacto en Sector Sanitario al utilizar plataformas antiguas diseñadas para la comunidad médica.
- **Presencia de muchos equipos basados en sistema operativo Windows XP en el sector.**

Orangeworm (abril 2018)

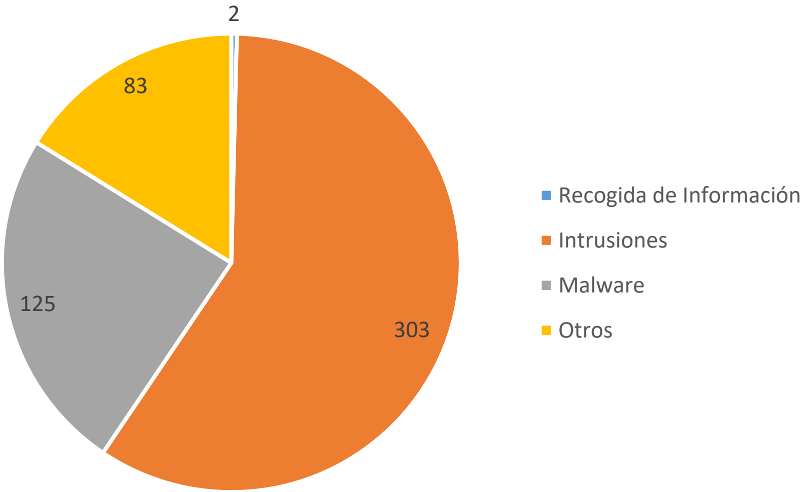
COMUNICACIÓN CON C&C

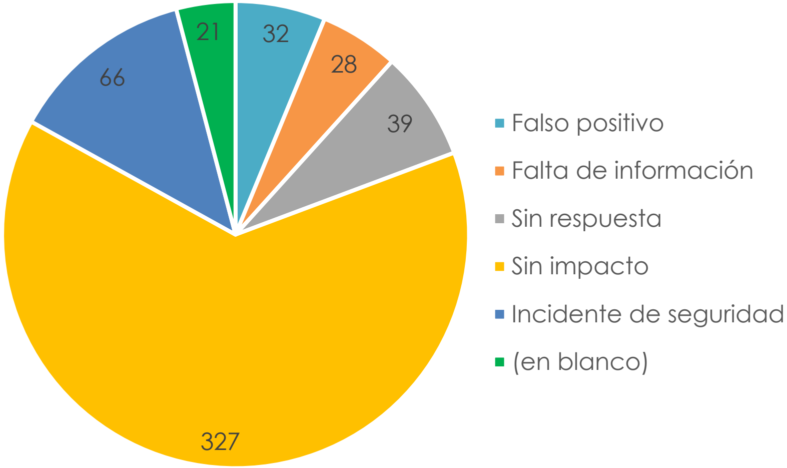
- Listado numeroso de servidores de mando y control.
- No hay ningún esfuerzo por cambiar los servidores de mando y control al propagarse por la red.
- Métodos de comunicación con los servidores C2 muy ruidosos
- **Objetivo muy blando.**

Incidentes gestionados en el sector salud

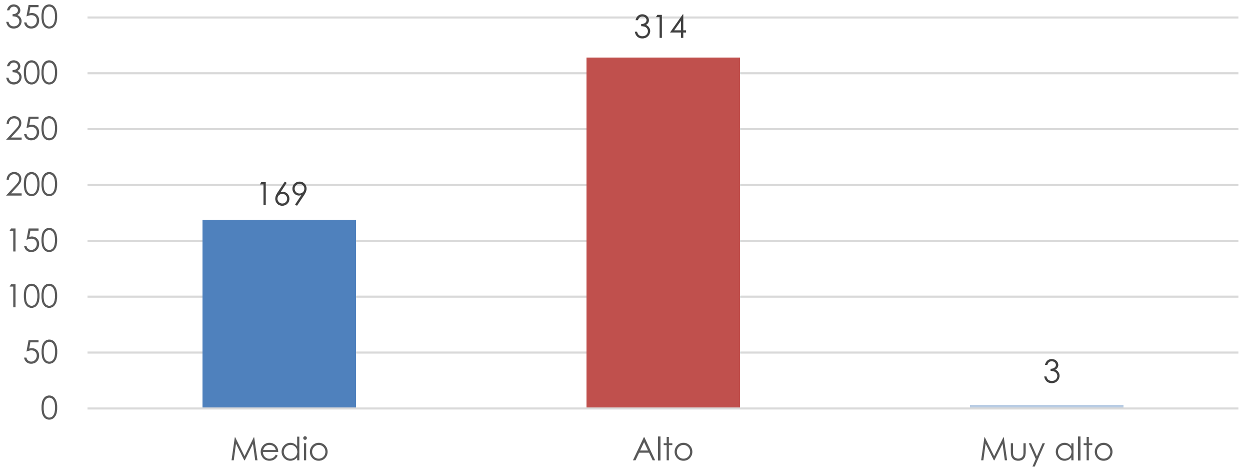


Incidentes gestionados en el sector salud





Incidentes gestionados en el sector salud



E-Mails

- **ccn@cni.es**
- ccn-cert@cni.es
- info@ccn-cert.cni.es
- sat-inet@ccn-cert.cni.es
- **lucia@ccn-cert.cni.es**
- organismo.certificacion@cni.es
- acreditacion.ccn@cni.es

Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- www.oc.ccn.cni.es

ORGANISMO DE CERTIFICACIÓN
CCN
Centro Criptológico Nacional
CCN-CERT
CIBERSEGURIDAD
EL BIENESTAR Y FUTURO DE NUESTRO PAÍS DEPENDE DE ELLO
MUY ALTO
CURSOS CCN-STIC
SERIES CCN-STIC
INFORMES
ALERTAS Y VULNERABILIDADES
EMPRESAS
SEGURIDAD AL DÍA

Gracias