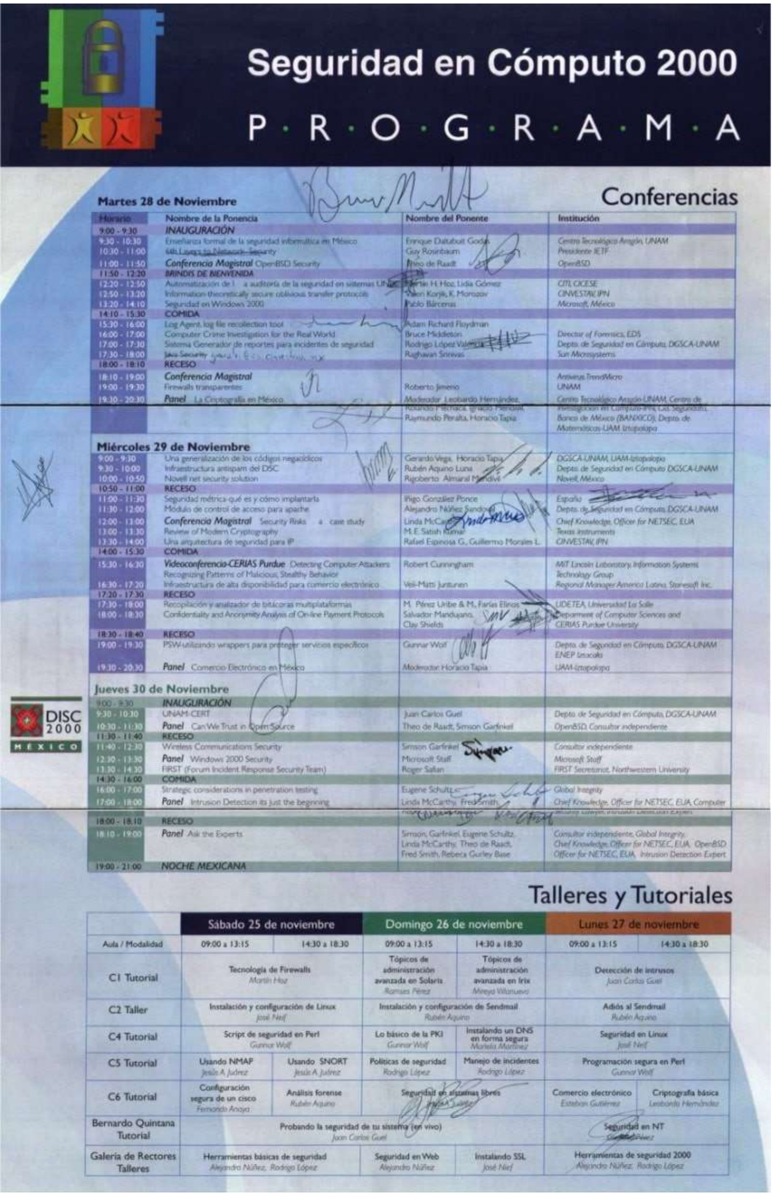
Protegiendo mis Dispositivos

Martín Hoz – mhoz@fortinet.com
VP de Ingeniería, Fortinet.

DISC
2020

UNAM
CERT

DGTIC
DIRECCIÓN GENERAL DE CÓMPUTO Y DE
TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN



Seguridad en Cómputo 2000

PROGRAMA

Conferencias

Martes 28 de Noviembre

Horario	Nombre de la Ponencia	Nombre del Ponente	Institución
9:00 - 9:30	*INAUGURACIÓN*		
9:30 - 10:30	Enseñanza formal de la seguridad informática en México	Enrique Daltabuit Godás	*Centro Tecnológico Aragón, UNAM*
10:30 - 11:00	~~6th Layers to Network Security~~	Guy Rosinbaum	*Presidente IETF*
11:00 - 11:50	*Conferencia Magistral* OpenBSD Security	Theo de Raadt	OpenBSD
11:50 - 12:20	*BRINDIS DE BIENVENIDA*		
12:20 - 12:50	Automatización de l a auditoría de la seguridad en sistemas UNIX	Martín H. Hoz, Lidia Gómez	*CITI, CICESE*
12:50 - 13:20	Information theoretically secure oblivious transfer protocols	Valeri Korjik, K. Morozov	*CINVESTAV, IPN*
13:20 - 14:10	Seguridad en Windows 2000	Pablo Bárcenas	*Microsoft, México*
14:10 - 15:30	COMIDA		
15:30 - 16:00	Log Agent, log file recolection tool	Adam Richard Floydman	
16:00 - 17:00	Computer Crime Investigation for the Real World	Bruce Middleton	*Director of Forensics, EDS*
17:00 - 17:30	Sistema Generador de reportes para incidentes de seguridad	Rodrigo López Valencia	*Depto. de Seguridad en Cómputo, DGSCA-UNAM*
17:30 - 18:00	~~Java Security~~ [illegible]	Raghavan Srinivas	*Sun Microsystems*
18:00 - 18:10	RECESO		
18:10 - 19:00	*Conferencia Magistral*		*Antivirus TrendMicro*
19:00 - 19:30	Firewalls transparentes	Roberto Jimeno	UNAM
19:30 - 20:30	*Panel* La Criptografía en México	*Moderador:* Leobardo Hernández, Rolando Menchaca, Ignacio Mendival, Raymundo Peralta, Horacio Tapia	*Centro Tecnológico Aragón-UNAM, Centro de Investigación en Computo-IPN, [illegible], Banco de México (BANXICO), Depto. de Matemáticas-UAM Iztapalapa*

Miércoles 29 de Noviembre

Horario	Nombre de la Ponencia	Nombre del Ponente	Institución
9:00 - 9:30	Una generalización de los códigos negacíclicos	Gerardo Vega, Horacio Tapia	*DGSCA-UNAM, UAM-Iztapalapa*
9:30 - 10:00	Infraestructura antispam del DSC	Rubén Aquino Luna	*Depto. de Seguridad en Cómputo DGSCA-UNAM*
10:00 - 10:50	Novell net security solution	Rigoberto Almaral Mendivil	*Novell, México*
10:50 - 11:00	RECESO		
11:00 - 11:30	Seguridad métrica qué es y cómo implantarla	Iñigo González Ponce	*España*
11:30 - 12:00	Módulo de control de acceso para apache	Alejandro Núñez Sandoval	*Depto. de Seguridad en Cómputo, DGSCA-UNAM*
12:00 - 13:00	*Conferencia Magistral* Security Risks a case study	Linda McCarthy	*Chief Knowledge Officer for NETSEC, EUA*
13:00 - 13:30	Review of Modern Cryptography	M. E. Satish Kumar	*Texas Instruments*
13:30 - 14:00	Una arquitectura de seguridad para IP	Rafael Espinosa G., Guillermo Morales L.	*CINVESTAV, IPN*
14:00 - 15:30	COMIDA		
15:30 - 16:30	*Videoconferencia-CERIAS Purdue* Detecting Computer Attackers Recognizing Patterns of Malicious, Stealthy Behavior	Robert Cunningham	*MIT Lincoln Laboratory, Information Systems Technology Group*
16:30 - 17:20	Infraestructura de alta disponibilidad para comercio electrónico	Veli-Matti Juntunen	*Regional Manager America Latina, Stonesoft Inc.*
17:20 - 17:30	RECESO		
17:30 - 18:00	Recopilación y analizador de bitácoras multiplataformas	M. Pérez Uribe & M. Farías Elinos	*UDETEA, Universidad La Salle*
18:00 - 18:30	Confidentiality and Anonymity Analysis of On-line Payment Protocols	Salvador Mandujano, Clay Shields	*Department of Computer Sciences and CERIAS Purdue University*
18:30 - 18:40	RECESO		
19:00 - 19:30	PSW-utilizando wrappers para proteger servicios específicos	Gunnar Wolf	*Depto. de Seguridad en Cómputo, DGSCA-UNAM ENEP Iztacala*
19:30 - 20:30	*Panel* Comercio Electrónico en México	*Moderador:* Horacio Tapia	*UAM-Iztapalapa*

Jueves 30 de Noviembre

Horario	Nombre de la Ponencia	Nombre del Ponente	Institución
9:00 - 9:30	*INAUGURACIÓN*		
9:30 - 10:30	UNAM-CERT	Juan Carlos Guel	*Depto. de Seguridad en Cómputo, DGSCA-UNAM*
10:30 - 11:30	*Panel* Can We Trust in Open Source	Theo de Raadt, Simson Garfinkel	*OpenBSD, Consultor independiente*
11:30 - 11:40	RECESO		
11:40 - 12:30	Wireless Communications Security	Simson Garfinkel	*Consultor independiente*
12:30 - 13:30	*Panel* Windows 2000 Security	Microsoft Staff	*Microsoft Staff*
13:30 - 14:30	FIRST (Forum Incident Response Security Team)	Roger Safian	*FIRST Secretariat, Northwestern University*
14:30 - 16:00	COMIDA		
16:00 - 17:00	Strategic considerations in penetration testing	Eugene Schultz	*Global Integrity*
17:00 - 18:00	*Panel* Intrusion Detection its just the beginning	Linda McCarthy, Fred Smith, [illegible]	*Chief Knowledge Officer for NETSEC, EUA, Computer Security Lawyer, Intrusion Detection Expert*
18:00 - 18:10	RECESO		
18:10 - 19:00	*Panel* Ask the Experts	Simson Garfinkel, Eugene Schultz, Linda McCarthy, Theo de Raadt, Fred Smith, Rebeca Gurley Base	*Consultor independiente, Global Integrity, Chief Knowledge Officer for NETSEC, EUA, OpenBSD Officer for NETSEC, EUA, Intrusion Detection Expert*
19:00 - 21:00	*NOCHE MEXICANA*		

DISC 2000 MÉXICO

Talleres y Tutoriales

	Sábado 25 de noviembre		Domingo 26 de noviembre		Lunes 27 de noviembre	
Aula / Modalidad	09:00 a 13:15	14:30 a 18:30	09:00 a 13:15	14:30 a 18:30	09:00 a 13:15	14:30 a 18:30
C1 Tutorial	Tecnología de Firewalls *Martín Hoz*		Tópicos de administración avanzada en Solaris *Ramses Pérez*	Tópicos de administración avanzada en Irix *Mireya Villanueva*	Detección de intrusos *Juan Carlos Guel*	
C2 Taller	Instalación y configuración de Linux *José Nieť*		Instalación y configuración de Sendmail *Rubén Aquino*		Adiós al Sendmail *Rubén Aquino*	
C4 Tutorial	Script de seguridad en Perl *Gunnar Wolf*		Lo básico de la PKI *Gunnar Wolf*	Instalando un DNS en forma segura *Mariela Martínez*	Seguridad en Linux *José Nieť*	
C5 Tutorial	Usando NMAP *Jesús A. Juárez*	Usando SNORT *Jesús A. Juárez*	Políticas de seguridad *Rodrigo López*	Manejo de incidentes *Rodrigo López*	Programación segura en Perl *Gunnar Wolf*	
C6 Tutorial	Configuración segura de un cisco *Fernando Anaya*	Análisis forense *Rubén Aquino*	Seguridad en sistemas libres *Jesús A. Juárez*		Comercio electrónico *Esteban Gutiérrez*	Criptografía básica *Leobardo Hernández*
Bernardo Quintana Tutorial	Probando la seguridad de tu sistema (en vivo) *Juan Carlos Guel*				Seguridad en NT *[illegible] Pérez*	
Galería de Rectores Talleres	Herramientas básicas de seguridad *Alejandro Núñez, Rodrigo López*		Seguridad en Web *Alejandro Núñez*	Instalando SSL *José Nieť*	Herramientas de seguridad 2000 *Alejandro Núñez, Rodrigo López*	

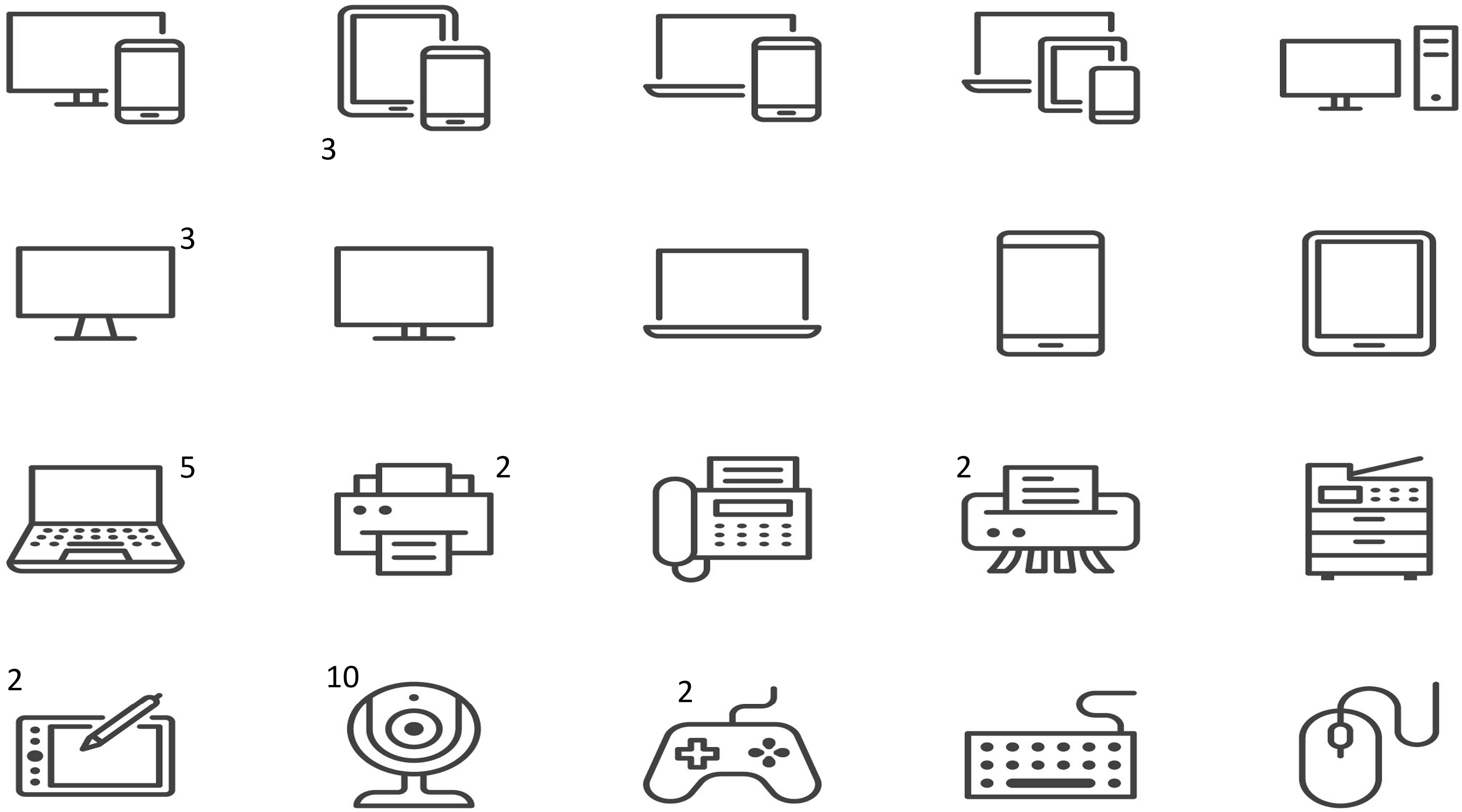
"No es lo mismo *Los 3 mosqueteros*..."

DISC
2020

DISC
2020

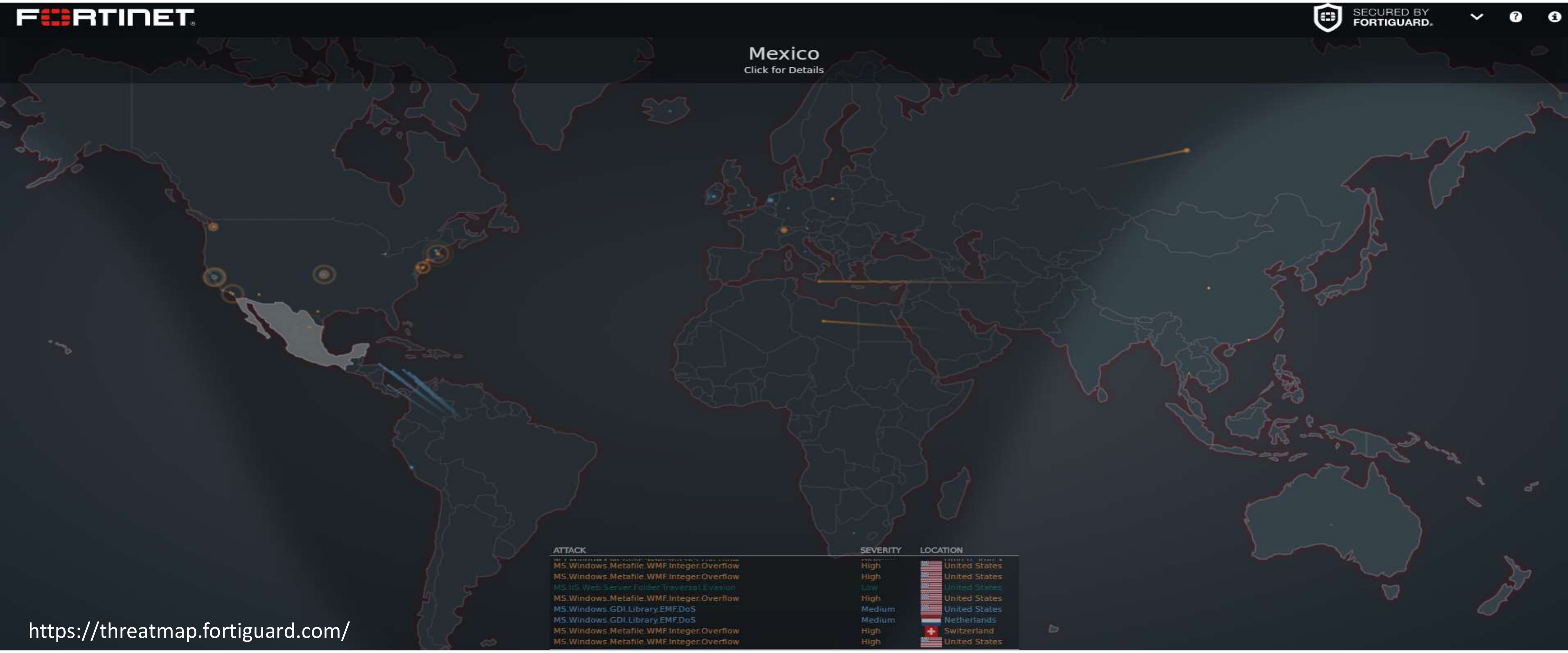
DISC 2020

DISC 2020



DISC
2020

Los ataques ocurren en todos lados.

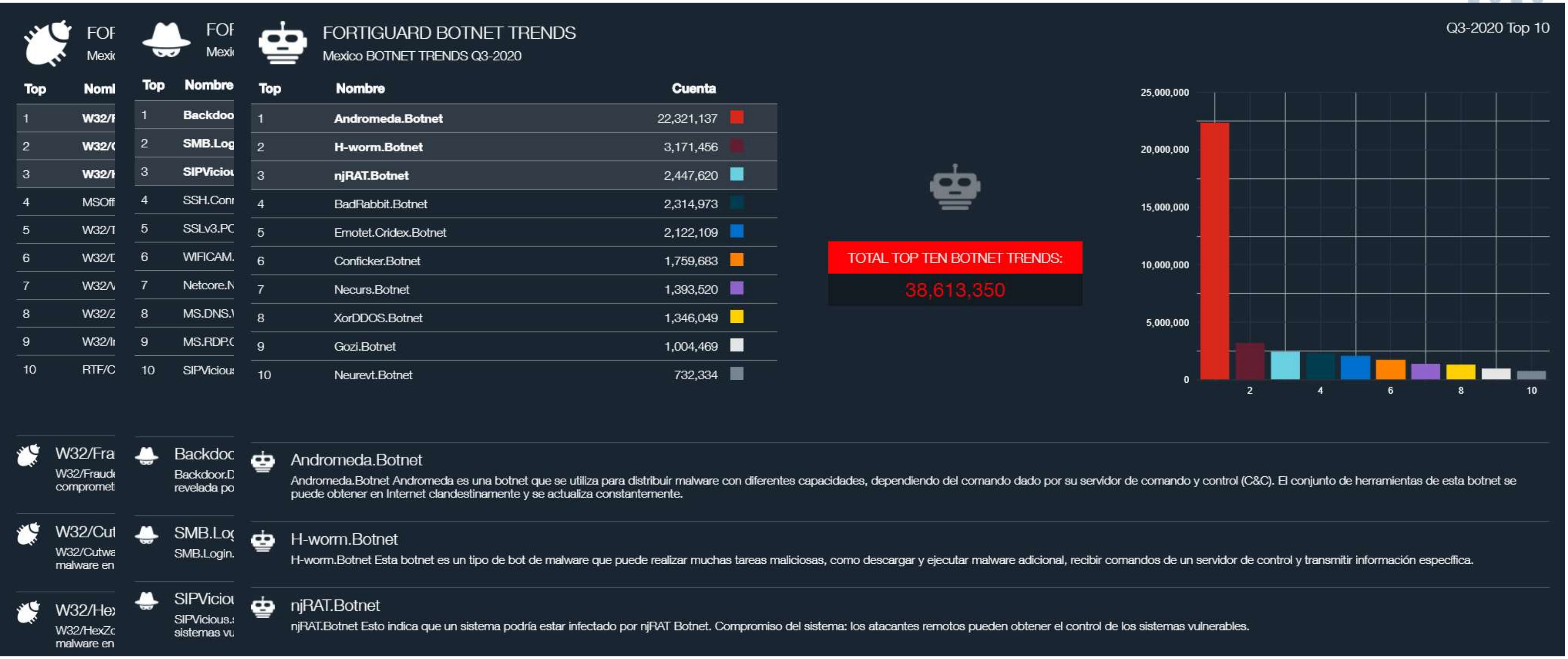


ATTACK	SEVERITY	LOCATION
MS.Windows.Metafile.WMF.Integer.Overflow	High	United States
MS.Windows.Metafile.WMF.Integer.Overflow	High	United States
MS.IIS.Web.Server.Folder.Traversal.Evasion	Low	United States
MS.Windows.Metafile.WMF.Integer.Overflow	High	United States
MS.Windows.GDI.Library.EMF.DoS	Medium	United States
MS.Windows.GDI.Library.EMF.DoS	Medium	Netherlands
MS.Windows.Metafile.WMF.Integer.Overflow	High	Switzerland
MS.Windows.Metafile.WMF.Integer.Overflow	High	United States

https://threatmap.fortiguard.com/

Ataques en México - 3er Trimestre 2020

https://www.fortinetthreatinsiderlat.com/es/Q3-2020/MX/html/trends#trends_position



FOF
Mexi

Top	Noml
1	**W32/F**
2	**W32/(**
3	**W32/I**
4	MSOff
5	W32/T
6	W32/D
7	W32/V
8	W32/Z
9	W32/I
10	RTF/C

FOF
Mexi

Top	Nombre
1	**Backdoo**
2	**SMB.Log**
3	**SIPViciou**
4	SSH.Conr
5	SSLv3.PC
6	WIFICAM.
7	Netcore.N
8	MS.DNS.\
9	MS.RDP.C
10	SIPVicious

FORTIGUARD BOTNET TRENDS

Mexico BOTNET TRENDS Q3-2020

Q3-2020 Top 10

Top	Nombre	Cuenta	
1	**Andromeda.Botnet**	22,321,137	🟥
2	**H-worm.Botnet**	3,171,456	🟥
3	**njRAT.Botnet**	2,447,620	🟦
4	BadRabbit.Botnet	2,314,973	■
5	Emotet.Cridex.Botnet	2,122,109	🟦
6	Conficker.Botnet	1,759,683	🟧
7	Necurs.Botnet	1,393,520	🟪
8	XorDDOS.Botnet	1,346,049	🟨
9	Gozi.Botnet	1,004,469	⬜
10	Neurevt.Botnet	732,334	■

TOTAL TOP TEN BOTNET TRENDS:

38,613,350

W32/Fra
W32/Fraud
compromet

Backdoc
Backdoor.D
revelada po

Andromeda.Botnet

Andromeda.Botnet Andromeda es una botnet que se utiliza para distribuir malware con diferentes capacidades, dependiendo del comando dado por su servidor de comando y control (C&C). El conjunto de herramientas de esta botnet se puede obtener en Internet clandestinamente y se actualiza constantemente.

W32/Cut
W32/Cutwa
malware en

SMB.Log
SMB.Login.

H-worm.Botnet

H-worm.Botnet Esta botnet es un tipo de bot de malware que puede realizar muchas tareas maliciosas, como descargar y ejecutar malware adicional, recibir comandos de un servidor de control y transmitir información específica.

W32/Hex
W32/HexZc
malware en

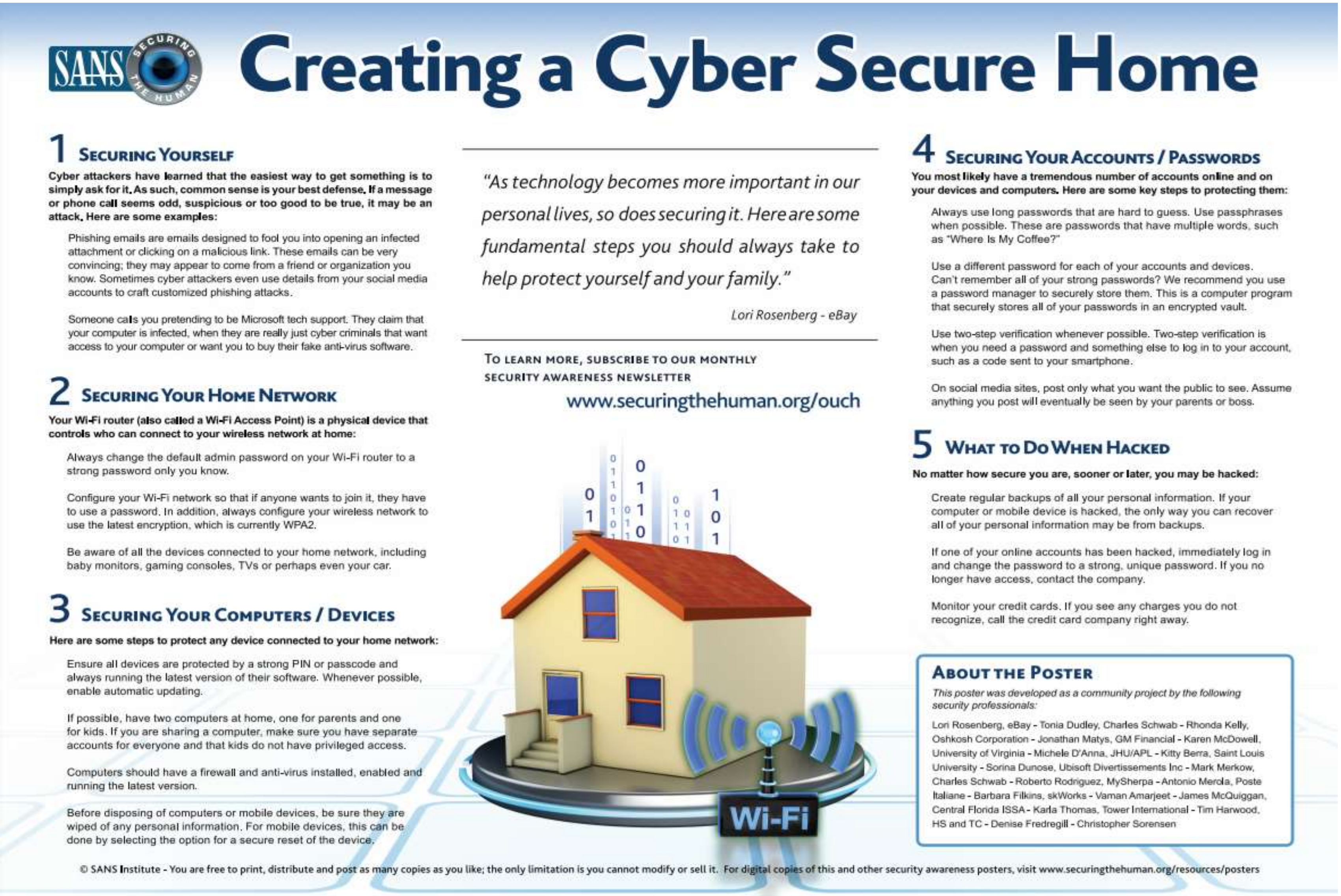
SIPViciou
SIPVicious.s
sistemas vu

njRAT.Botnet

njRAT.Botnet Esto indica que un sistema podría estar infectado por njRAT Botnet. Compromiso del sistema: los atacantes remotos pueden obtener el control de los sistemas vulnerables.

"¡Que no panda el cúnico!" - CH

DISC 2020



Creating a Cyber Secure Home

1 Securing Yourself

Cyber attackers have learned that the easiest way to get something is to simply ask for it. As such, common sense is your best defense. If a message or phone call seems odd, suspicious or too good to be true, it may be an attack. Here are some examples:

Phishing emails are emails designed to fool you into opening an infected attachment or clicking on a malicious link. These emails can be very convincing; they may appear to come from a friend or organization you know. Sometimes cyber attackers even use details from your social media accounts to craft customized phishing attacks.

Someone cals you pretending to be Microsoft tech support. They claim that your computer is infected, when they are really just cyber criminals that want access to your computer or want you to buy their fake anti-virus software.

2 Securing Your Home Network

Your Wi-Fi router (also called a Wi-Fi Access Point) is a physical device that controls who can connect to your wireless network at home:

Always change the default admin password on your Wi-Fi router to a strong password only you know.

Configure your Wi-Fi network so that if anyone wants to join it, they have to use a password. In addition, always configure your wireless network to use the latest encryption, which is currently WPA2.

Be aware of all the devices connected to your home network, including baby monitors, gaming consoles, TVs or perhaps even your car.

3 Securing Your Computers / Devices

Here are some steps to protect any device connected to your home network:

Ensure all devices are protected by a strong PIN or passcode and always running the latest version of their software. Whenever possible, enable automatic updating.

If possible, have two computers at home, one for parents and one for kids. If you are sharing a computer, make sure you have separate accounts for everyone and that kids do not have privileged access.

Computers should have a firewall and anti-virus installed, enabled and running the latest version.

Before disposing of computers or mobile devices, be sure they are wiped of any personal information. For mobile devices, this can be done by selecting the option for a secure reset of the device.

> *"As technology becomes more important in our personal lives, so does securing it. Here are some fundamental steps you should always take to help protect yourself and your family."*
>
> *Lori Rosenberg - eBay*

To learn more, subscribe to our monthly security awareness newsletter

www.securingthehuman.org/ouch

4 Securing Your Accounts / Passwords

You most likely have a tremendous number of accounts online and on your devices and computers. Here are some key steps to protecting them:

Always use long passwords that are hard to guess. Use passphrases when possible. These are passwords that have multiple words, such as "Where Is My Coffee?"

Use a different password for each of your accounts and devices. Can't remember all of your strong passwords? We recommend you use a password manager to securely store them. This is a computer program that securely stores all of your passwords in an encrypted vault.

Use two-step verification whenever possible. Two-step verification is when you need a password and something else to log in to your account, such as a code sent to your smartphone.

On social media sites, post only what you want the public to see. Assume anything you post will eventually be seen by your parents or boss.

5 What to Do When Hacked

No matter how secure you are, sooner or later, you may be hacked:

Create regular backups of all your personal information. If your computer or mobile device is hacked, the only way you can recover all of your personal information may be from backups.

If one of your online accounts has been hacked, immediately log in and change the password to a strong, unique password. If you no longer have access, contact the company.

Monitor your credit cards. If you see any charges you do not recognize, call the credit card company right away.

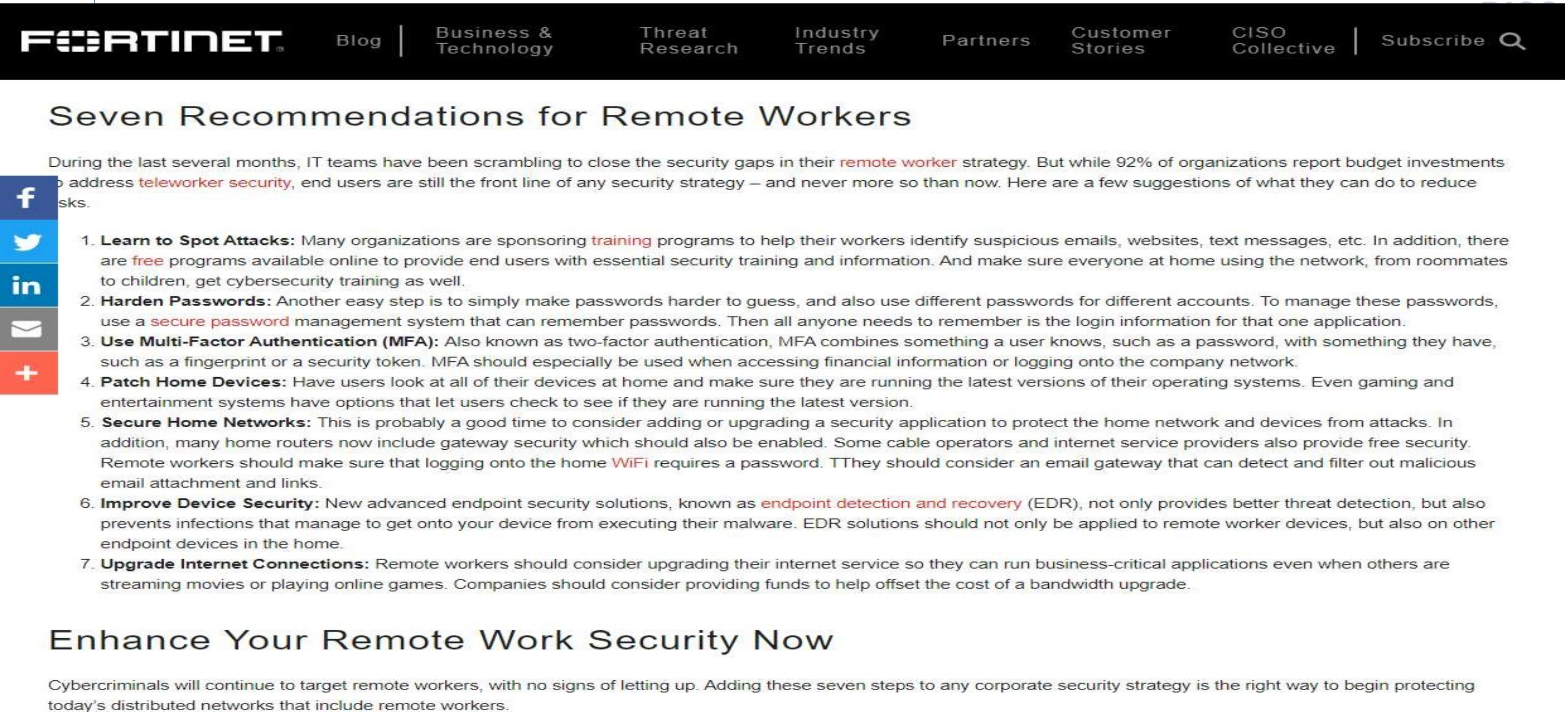
About the Poster

This poster was developed as a community project by the following security professionals:

Lori Rosenberg, eBay - Tonia Dudley, Charles Schwab - Rhonda Kelly, Oshkosh Corporation - Jonathan Matys, GM Financial - Karen McDowell, University of Virginia - Michele D'Anna, JHU/APL - Kitty Berra, Saint Louis University - Sorina Dunose, Ubisoft Divertissements Inc - Mark Merkow, Charles Schwab - Roberto Rodriguez, MySherpa - Antonio Merola, Poste Italiane - Barbara Filkins, skWorks - Vaman Amarjeet - James McQuiggan, Central Florida ISSA - Karla Thomas, Tower International - Tim Harwood, HS and TC - Denise Fredregill - Christopher Sorensen

For digital copies of this and other security awareness posters, visit www.securingthehuman.org/resources/posters

https://www.sans.org/security-resources/posters/creating-cyber-secure-home/80/download https://www.fortinet.com/blog/industry-trends/tips-for-staying-secure-while-working-from-home



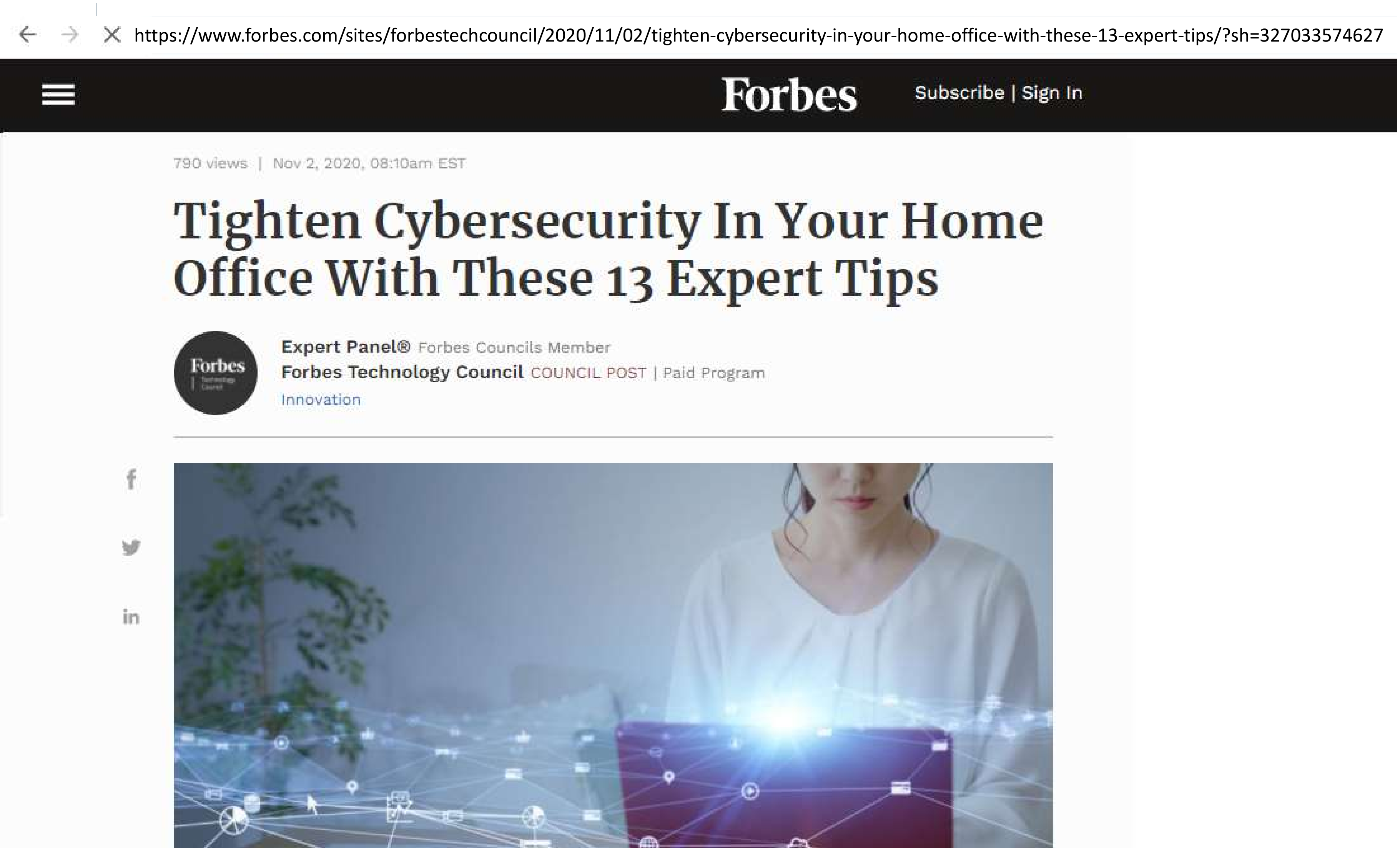
Seven Recommendations for Remote Workers

During the last several months, IT teams have been scrambling to close the security gaps in their remote worker strategy. But while 92% of organizations report budget investments o address teleworker security, end users are still the front line of any security strategy – and never more so than now. Here are a few suggestions of what they can do to reduce sks.

1. **Learn to Spot Attacks:** Many organizations are sponsoring training programs to help their workers identify suspicious emails, websites, text messages, etc. In addition, there are free programs available online to provide end users with essential security training and information. And make sure everyone at home using the network, from roommates to children, get cybersecurity training as well.
2. **Harden Passwords:** Another easy step is to simply make passwords harder to guess, and also use different passwords for different accounts. To manage these passwords, use a secure password management system that can remember passwords. Then all anyone needs to remember is the login information for that one application.
3. **Use Multi-Factor Authentication (MFA):** Also known as two-factor authentication, MFA combines something a user knows, such as a password, with something they have, such as a fingerprint or a security token. MFA should especially be used when accessing financial information or logging onto the company network.
4. **Patch Home Devices:** Have users look at all of their devices at home and make sure they are running the latest versions of their operating systems. Even gaming and entertainment systems have options that let users check to see if they are running the latest version.
5. **Secure Home Networks:** This is probably a good time to consider adding or upgrading a security application to protect the home network and devices from attacks. In addition, many home routers now include gateway security which should also be enabled. Some cable operators and internet service providers also provide free security. Remote workers should make sure that logging onto the home WiFi requires a password. TThey should consider an email gateway that can detect and filter out malicious email attachment and links.
6. **Improve Device Security:** New advanced endpoint security solutions, known as endpoint detection and recovery (EDR), not only provides better threat detection, but also prevents infections that manage to get onto your device from executing their malware. EDR solutions should not only be applied to remote worker devices, but also on other endpoint devices in the home.
7. **Upgrade Internet Connections:** Remote workers should consider upgrading their internet service so they can run business-critical applications even when others are streaming movies or playing online games. Companies should consider providing funds to help offset the cost of a bandwidth upgrade.

Enhance Your Remote Work Security Now

Cybercriminals will continue to target remote workers, with no signs of letting up. Adding these seven steps to any corporate security strategy is the right way to begin protecting today's distributed networks that include remote workers.



https://www.forbes.com/sites/forbestechcouncil/2020/11/02/tighten-cybersecurity-in-your-home-office-with-these-13-expert-tips/?sh=327033574627

790 views | Nov 2, 2020, 08:10am EST

Tighten Cybersecurity In Your Home Office With These 13 Expert Tips

Expert Panel® Forbes Councils Member
Forbes Technology Council COUNCIL POST | Paid Program
Innovation

Higiene Digital

- Antivirus/ Firewall personal/ AntiMalware/ IPS-WCF /xDR
- Siempre actualizar
  - Sistema Operativo y protección
  - Firmware, TV, Impresoras, …
- Siempre cambiar defaults
  - Contraseñas, niveles de seguridad. Equipos y red.
- Menos privilegios

Cuidados mínimos al usar tecnología

- No confiarse de extraños
  - Sean personas o programas
  - *Hardening* de Apps
  - Solo redes confiables
- Respaldar siempre
  - Siempre duplicados
  - En medios fuera de línea
- Separar responsabilidades
  - Personal vs Trabajo
  - Público vs Privado
  - “Necesidad de conocer”

¡Ahí viene el hacker!

DISC 2020

Bugs / Vulnerabilidades
Nuevas formas de ataque
Ataques exitosos

¡Diligencia y responsabilidad!

Plataforma de ciberseguridad para la superficie de ataque digital

Dispositivo

Máquina Virtual

Nube

Seguridad-como-Servicio

Software

Acceso de Red con Confianza Cero

- Protección del Punto terminal
- Token
- Control de Acceso a la Red (NAC)
- Gestión de Identidad
- Nube fuera de la red

Redes basadas en Seguridad

- NP7 Alto Desempeño
- FireWall de Próxima Generación
- SD-WAN + SD-Branch
- Switch
- Access Point
- Extensores

Seguridad dinámica para nube

- Máquinas Virtuales
- Nube Privada
- SaaS
- CASB
- Chassis de Alto Desempeño
- WAF

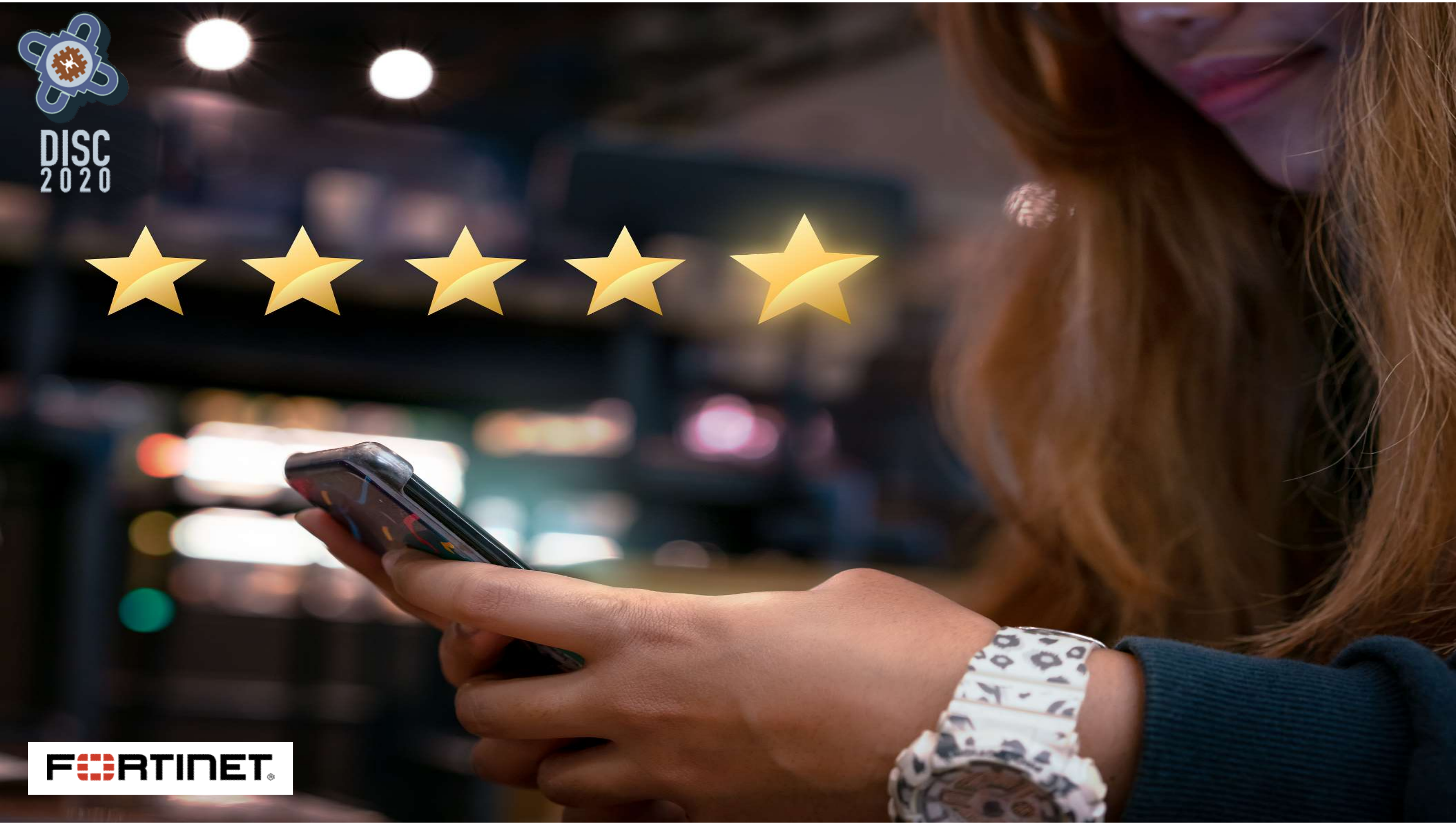
Gestión de Seguridad basada en IA

- Reportes
- SIEM
- SOAR
- Sandbox
- Deceptor
- Analista Virtual de SOC
- Análisis de Comportamiento
- Protección de Punto Terminal
- EDR / xDR

Centro de Gestión Completa

- Conectores / APIs
- Gestión Central
- Gestión en Nube
- Inspección en Nube
- Soporte
- Comunidad de Desarrolladores

FORTINET


DISC
2020
FORTINET

¡ Muchas gracias !

¿ Preguntas ?

DISC
2020

FORTINET

Martín Hoz
mhoz@fortinet.com