ONLINE

INFOSECURITY SUMMIT

Estado actual de la seguridad en México y Latinoamérica

Miguel Ángel Mendoza
Security Researcher ESET LATAM

infosecurity® MEXICO

En alianza con

ISACA. Mexico City Chapter

ISACA. Guadalajara Chapter

Organizado por Reed Exhibitions®

Ciberseguridad en el orbe

Ciberataques

Diez mayores riesgos que enfrenta el mundo en 2020

Fuente: World Economic Forum's Global Risks Report

Top 10 risks in terms of

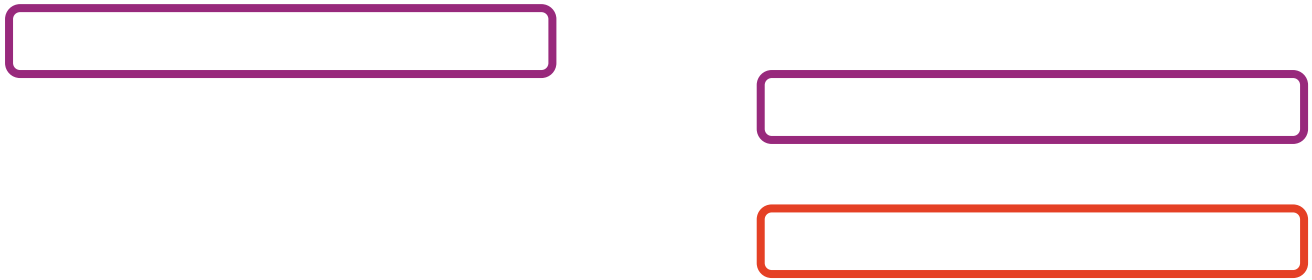
Likelihood

Top 10 risks in terms of

Impact

Categories

- Economic
- Environmental
- Geopolitical
- Societal
- Technological



Fuente: World Economic Forum's Global Risks Report

Ciberataques

Mayor posibilidad de ocurrir y consecuencias más graves

welivesecurity™ BY ESET®

Crecen los ataques de ransomware dirigidos a hospitales, asegura INTERPOL

INTERPOL detectó un crecimiento significativo en el número de intentos de ataques de ransomware dirigidos a instituciones e infraestructuras que juegan un rol clave en la lucha contra el coronavirus.

6 Apr 2020

Fuente: WeLiveSecurity

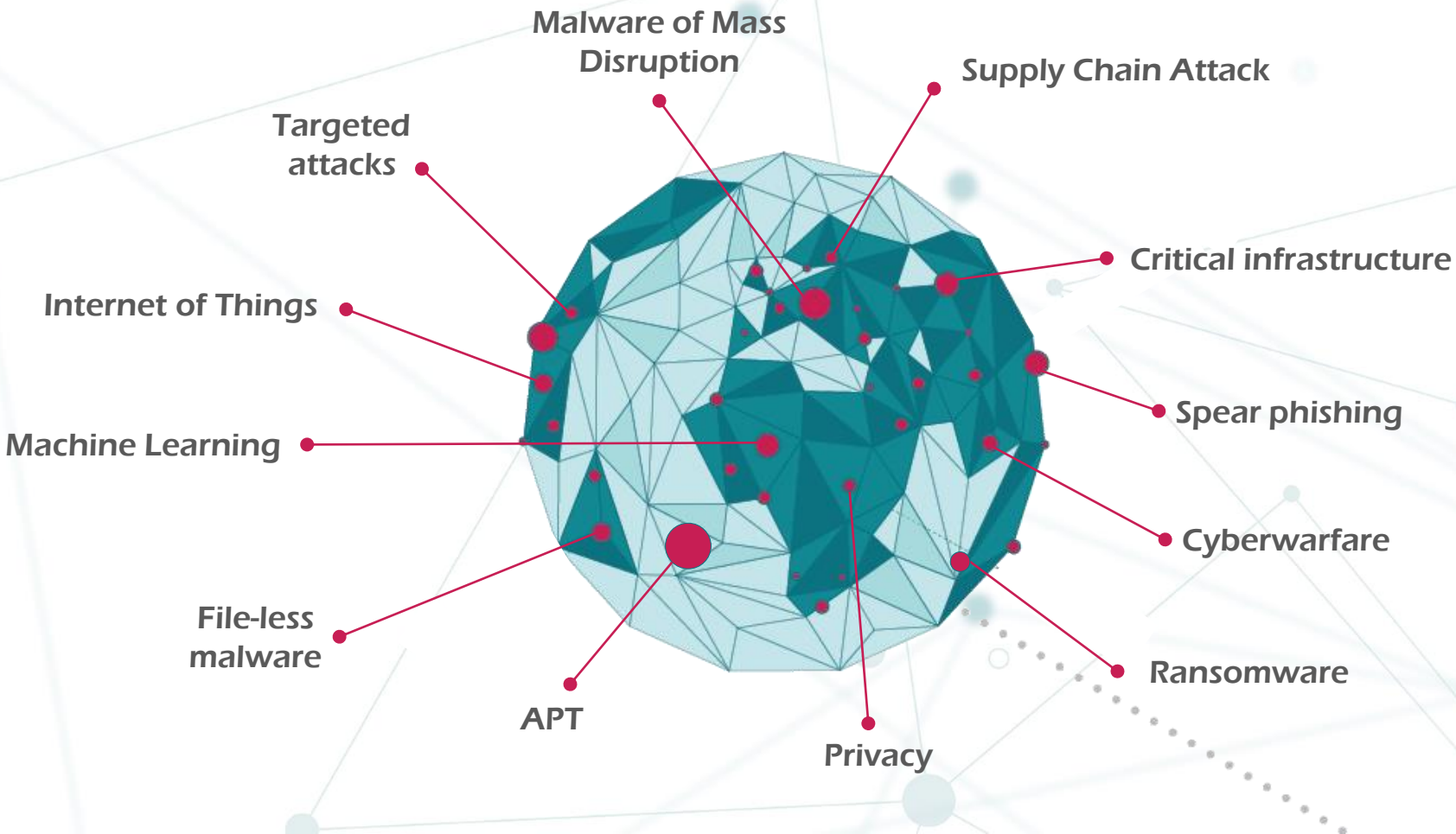
welivesecurity™ BY ESET®

Llamado de líderes mundiales para detener los ciberataques al sector salud

Más de 40 líderes mundiales llaman a los gobiernos a tomar medidas para detener los ciberataques a instituciones vinculadas con el sector de la salud en el contexto actual por la pandemia del COVID-19.

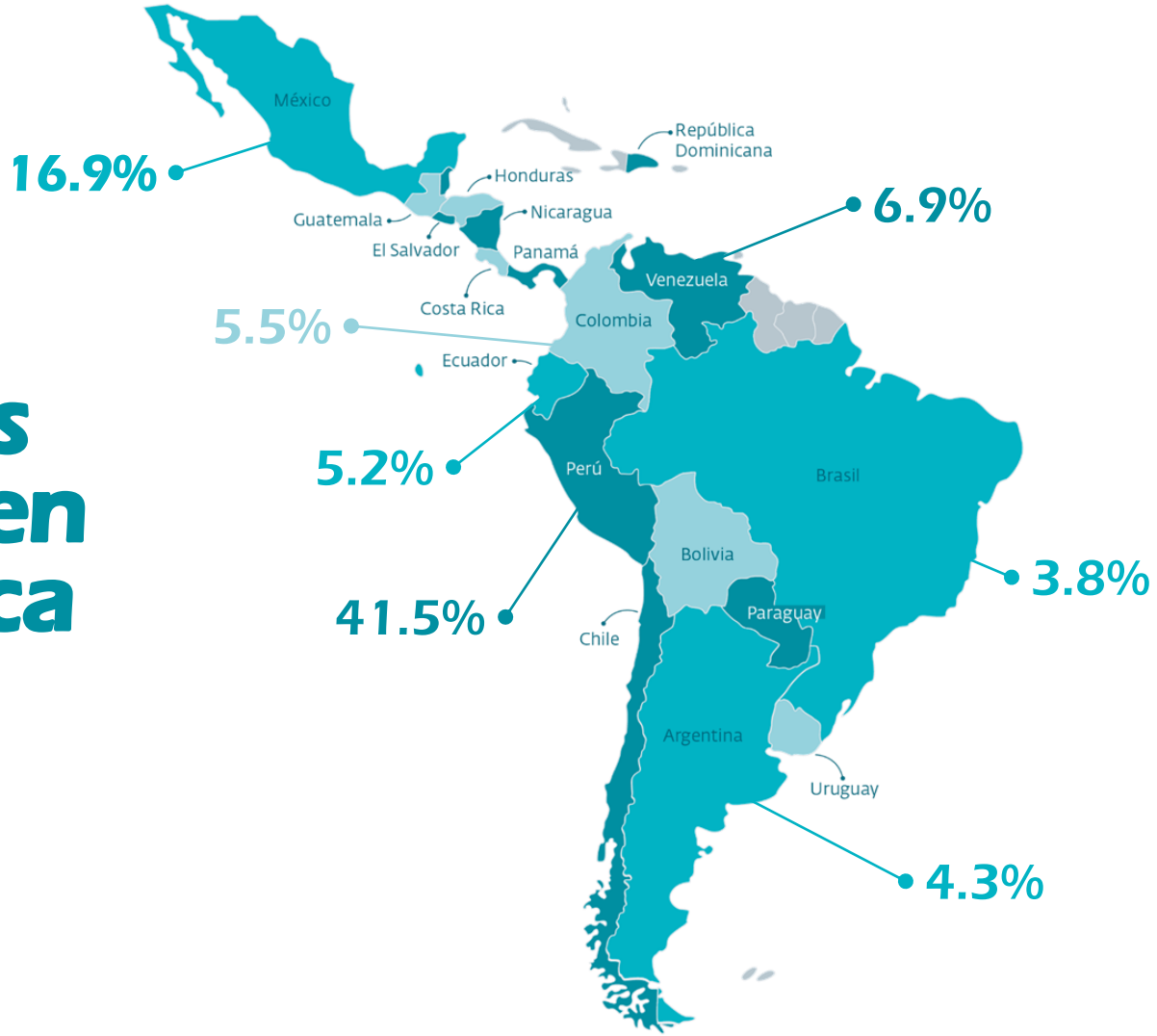
27 May 2020

Fuente: WeLiveSecurity


Malware of Mass Disruption
Supply Chain Attack
Targeted attacks
Critical infrastructure
Internet of Things
Spear phishing
Machine Learning
Cyberwarfare
File-less malware
Ransomware
APT
Privacy

Riesgos globales, riesgos regionales

Detecciones de malware en Latinoamérica



Campañas maliciosas en Latinoamérica

VictoryGate: ESET disrumpe botnet utilizada para minar criptomonedas que afecta principalmente a Perú

ESET descubre y disrumpe parte de la operación de VictoryGate, una botnet compuesta principalmente por equipos comprometidos en Perú, utilizada para minar criptomonedas.

Machete sigue activo realizando ciberespionaje en Latinoamérica

Investigación de ESET devela que los operadores detrás del malware Machete siguen activos y realizando operaciones de ciberespionaje dirigidas a organismos gubernamentales de Ecuador, Colombia, Nicaragua y Venezuela.

Campañas maliciosas en Latinoamérica

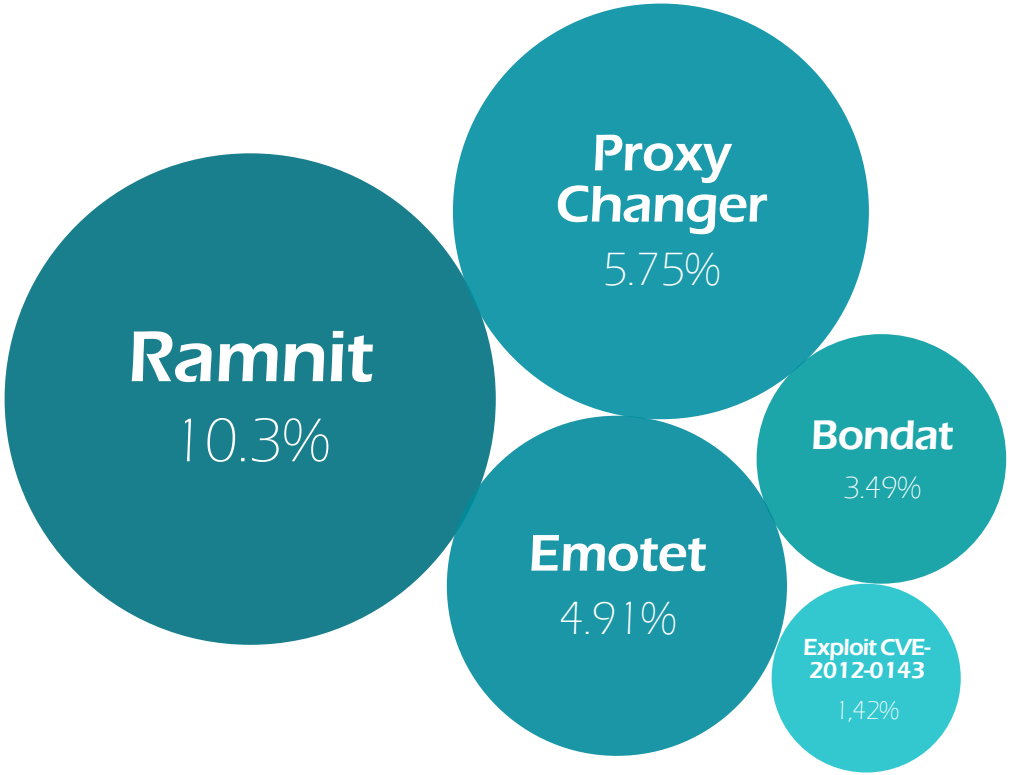
Campañas maliciosas de múltiples etapas afectan a usuarios de Chile

Un análisis técnico sobre la botnet Mekioto en campañas que afectan a países de la región y que tiene como principal objetivo robar información financiera de sus víctimas.

Casbaneiro: particularidades de este troyano bancario que afecta a Brasil y México

Investigación de ESET muestra la actividad de troyanos bancarios en América Latina. Presentamos el análisis técnico de Casbaneiro, un banker que hace uso de diversas técnicas para ocultar la dirección de su servidor de C&C.

Amenazas más detectadas en Latinoamérica



ONLINE

INFOSECURITY SUMMIT

infosecurity MEXICO

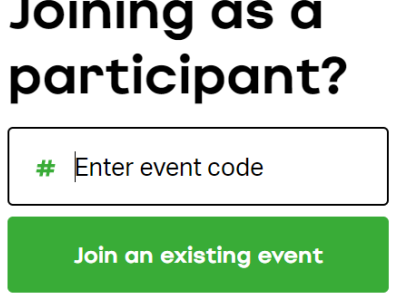
En alianza con ISACA Mexico City Chapter ISACA Guadalajara Chapter

SLIDO será la herramienta que te permitirá interactuar durante el evento, podrás escribir tus dudas y comentarios para la sesión de preguntas y respuestas al final

1

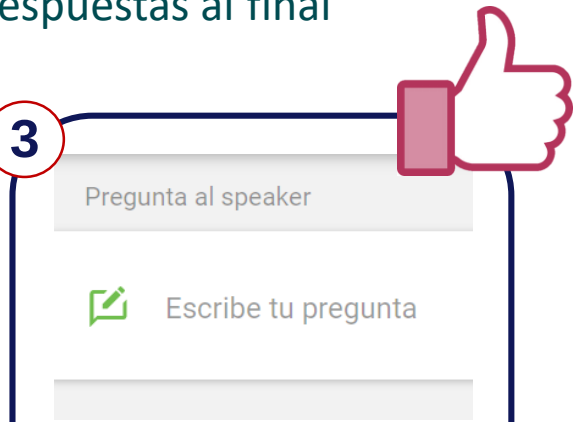
Ingresa a www.slido.com o escanea desde tu celular el código QR.

2



Ingresa el código infosec2020 y da clic en Join an existing event

3

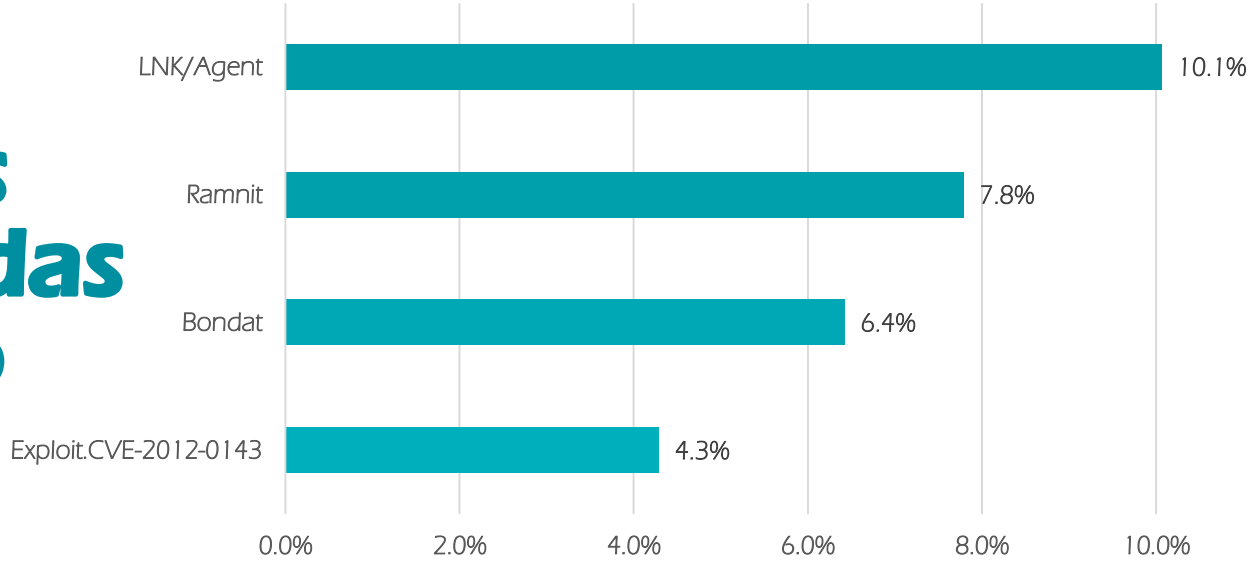


¡Listo!

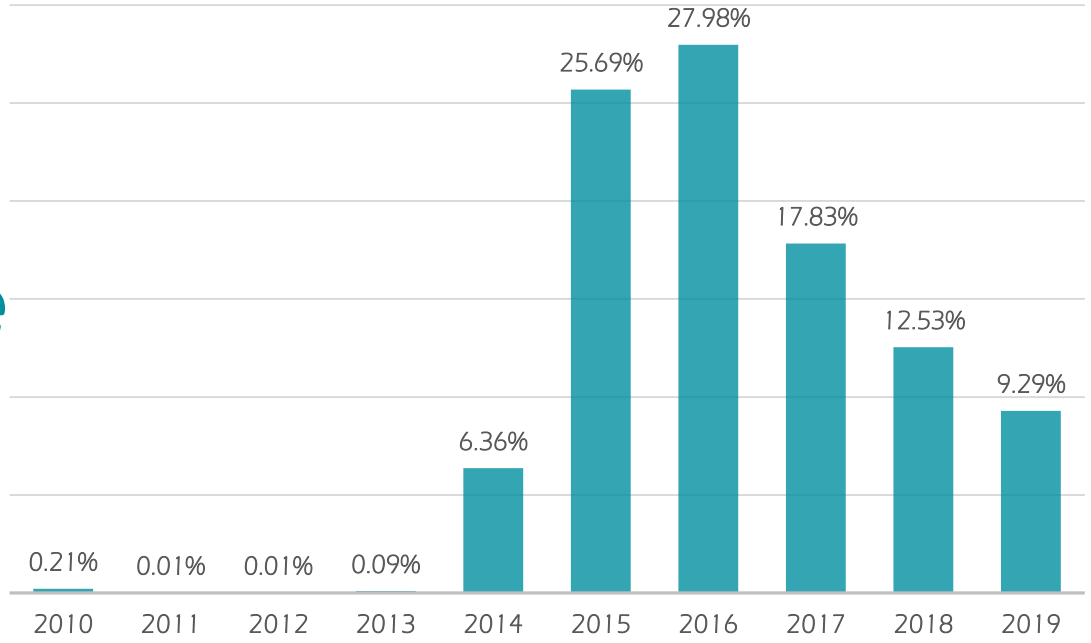
Inicia respondiendo las 4 preguntas que aparecerán en pantalla

Riesgos regionales, riesgos locales

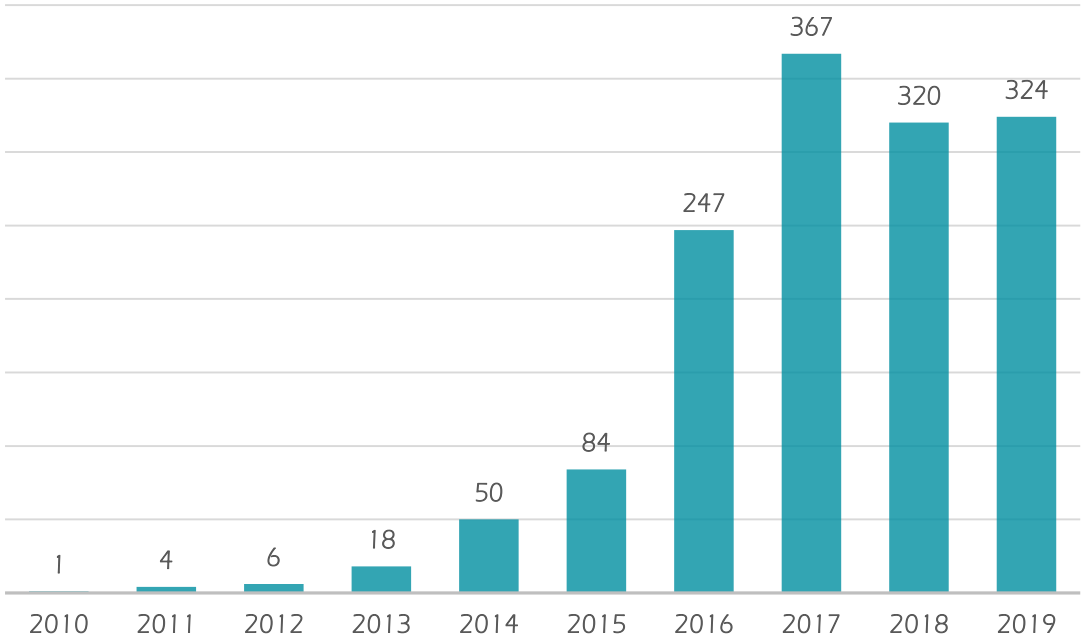
Amenazas más detectadas en México



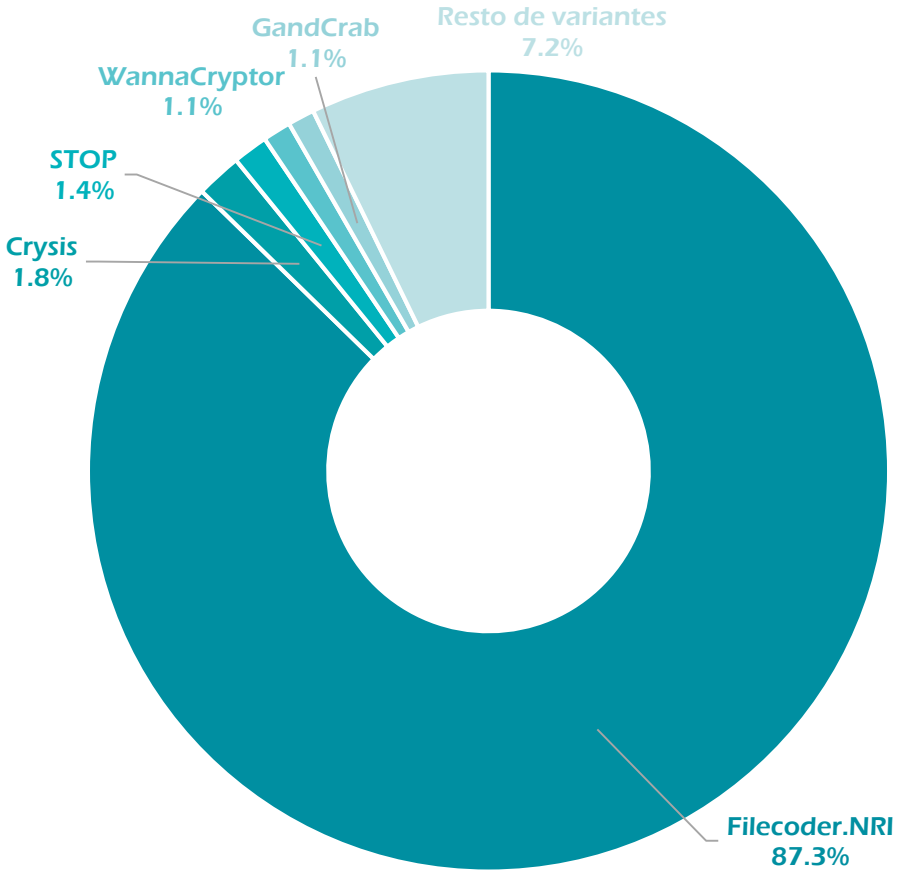
Detecciones de ransomware en México



Familias de ransomware en México



Familias de ransomware en México



welivesecurity™ BY ESET®

Ciberataque a Pemex afectó el 5% de las computadoras

Ataque dirigido hacia Petróleos Mexicanos (Pemex) comprometió el 5% de los equipos, pero la compañía aseguró que esto no afectó a sus sistemas y que opera con normalidad

12 Nov 2019

Fuente: WeLiveSecurity


Prevención
Predicción
Detección
Respuesta

Más información, mayor protección

MITRE ATT&CK™

Acceso inicial	Ejecución	Persistencia	Escalación de privilegios	Evasión de defensas	Acceso a credenciales	Identificación	Movimiento lateral	Recolección de información	Comando y control	Exfiltración	Impacto
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Application Access Token	Bash History	Application Window Discovery	Application Access Token	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Application Deployment Software	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	BITS Jobs	Cloud Instance Metadata API	Cloud Service Dashboard		Data from Cloud Storage Object	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media		AppInit DLLs	Application Shimming	Bypass User Account Control	Credential Dumping	Cloud Service Discovery	Component Object Model and Distributed COM	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Component Object Model and Distributed COM	Application Shimming	Bypass User Account Control	Clear Command History	Credentials from Web Browsers	Domain Trust Discovery	Exploitation of Remote Services	Data from Local System	Data Encoding		Disk Structure Wipe
Spearphishing Link	Control Panel Items	Authentication Package	DLL Search Order Hijacking	CMSTP	Credentials in Files	File and Directory Discovery	Internal Spearphishing	Data from Network Shared Drive	Data Obfuscation	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing via Service	Dynamic Data Exchange	BITS Jobs	Dylib Hijacking	Code Signing	Credentials in Registry	Network Service Scanning	Logon Scripts	Data from Removable Media	Domain Fronting	Exfiltration Over Other Network Medium	Firmware Corruption
Supply Chain Compromise	Execution through API	Bootkit	Elevated Execution with Prompt	Compile After Delivery	Exploitation for Credential Access	Network Share Discovery	Pass the Hash	Data Staged	Domain Generation Algorithms	Exfiltration Over Physical Medium	Inhibit System Recovery
Trusted Relationship	Execution through Module Load	Browser Extensions	Emond	Compiled HTML File	Forced Authentication	Network Sniffing	Pass the Ticket	Email Collection	Fallback Channels	Scheduled Transfer	Network Denial of Service
Valid Accounts	Exploitation for Client Execution	Change Default File Association	Exploitation for Privilege Escalation	Component Firmware	Hooking	Password Policy Discovery	Remote Desktop Protocol	Input Capture	Multi-hop Proxy	Transfer Data to Cloud Account	Resource Hijacking
	Graphical User Interface	Component Firmware	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Peripheral Device Discovery	Remote File Copy	Man in the Browser	Multi-Stage Channels		Runtime Data Manipulation
	InstallUtil	Component Object Model Hijacking	File System Permissions Weakness	Connection Proxy	Input Prompt	Permission Groups Discovery	Remote Services	Screen Capture	Multiband Communication		Service Stop
	Launchctl	Create Account	Hooking	Control Panel Items	Kerberoasting	Process Discovery	Replication Through Removable Media	Video Capture	Multilayer Encryption		Stored Data Manipulation
	Local Job Scheduling	DLL Search Order Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	Shared Webroot		Port Knocking		System Shutdown/Reboot
	LSASS Driver	Dylib Hijacking	Launch Daemon	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	SSH Hijacking		Remote Access Tools		Transmitted Data Manipulation
	Mshta	Emond	New Service	Disabling Security Tools	Network Sniffing	Security Software Discovery	Taint Shared Content		Remote File Copy		
	PowerShell	External Remote Services	Parent PID Spoofing	DLL Search Order Hijacking	Password Filter DLL	Software Discovery	Third-party Software		Standard Application Layer Protocol		
	Regsvcs/Regasm	File System Permissions Weakness	Path Interception	DLL Side-Loading	Private Keys	System Information Discovery	Web Session Cookie		Standard Cryptographic Protocol		
	Regsvr32	Hidden Files and Directories	Plist Modification	Execution Guardrails	Securityd Memory	System Network Configuration Discovery	Windows Admin Shares		Standard Non-Application Layer Protocol		
	Rundll32	Hooking	Port Monitors	Exploitation for Defense Evasion	Steal Application Access Token	System Network Connections Discovery	Windows Remote Management		Uncommonly Used Port		
	Scheduled Task	Hypervisor	PowerShell Profile	Extra Window Memory Injection	Steal Web Session Cookie	System Owner/User Discovery			Web Service		
	Scripting	Image File Execution Options Injection	Process Injection	File and Directory Permissions Modification	Two-Factor Authentication Interception	System Service Discovery					
	Service Execution	Implant Container Image	Scheduled Task	File Deletion		System Time Discovery					
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Service Registry Permissions Weakness	File System Logical Offsets		Virtualization/Sandbox Evasion					
	Signed Script Proxy Execution	Launch Agent	Setuid and Setgid	Gatekeeper Bypass							
	Source	Launch Daemon	SID-History Injection	Group Policy Modification							
	Space after Filename	Launchctl	Startup Items	Hidden Files and Directories							
	Third-party Software	LC_LOAD_DYLIB Addition	Sudo	Hidden Users							
	Trap	Local Job Scheduling	Sudo Caching	Hidden Window							
	Trusted Developer Utilities	Login Item	Valid Accounts	HISTCONTROL							
	User Execution	Logon Scripts	Web Shell	Image File Execution Options Injection							
	Windows Management Instrumentation	LSASS Driver		Indicator Blocking							
	Windows Remote Management	Modify Existing Service		Indicator Removal from Tools							
	XSL Script Processing	Netsh Helper DLL		Indicator Removal on Host							
		New Service		Indirect Command Execution							
		Office Application Startup		Install Root Certificate							
		Path Interception		InstallUtil							
		Plist Modification		Launchctl							
		Port Knocking		LC_MAIN Hijacking							
		Port Monitors		Masquerading							
		PowerShell Profile		Modify Registry							
		Rc.common		Mshta							
		Re-opened Applications		Network Share Connection Removal							
		Redundant Access		NTFS File Attributes							
		Registry Run Keys / Startup Folder		Obfuscated Files or Information							
		Scheduled Task		Parent PID Spoofing							
		Screensaver		Plist Modification							
		Security Support Provider		Port Knocking							
		Server Software Component		Process Doppelgänging							
		Service Registry Permissions Weakness		Process Hollowing							
		Setuid and Setgid		Process Injection							
		Shortcut Modification		Redundant Access							
		SIP and Trust Provider Hijacking		Regsvcs/Regasm							
		Startup Items		Regsvr32							
		System Firmware		Revert Cloud Instance							
		Systemd Service		Rootkit							
		Time Providers		Rundll32							
		Trap		Scripting							
		Valid Accounts		Signed Binary Proxy Execution							
		Web Shell		Signed Script Proxy Execution							
		Windows Management Instrumentation Event Subscription		SIP and Trust Provider Hijacking							
		Winlogon Helper DLL		Software Packing							
				Space after Filename							
				Template Injection							
				Timestomp							
				Trusted Developer Utilities							
				Unused/Unsupported Cloud Regions							
				Valid Accounts							
				Virtualization/Sandbox Evasion							
				Web Service							
				Web Session Cookie							
				XSL Script Processing							

MITRE | ATT&CK™

Acceso inicial

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Replication Through Removable Media
- Spearphishing Attachment
- Spearphishing Link
- Spearphishing via Service
- Supply Chain Compromise
- Trusted Relationship
- Valid Accounts

MITRE ATT&CK® Navigator

__Amavaldo x __Casbaneiro x __Grandoreiro x __Guildma x __Machete x __Mispadu x __Remtasu x __VictoryGate x __Others x +

selection controls | layer controls | technique controls

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	34 items	62 items	32 items	69 items	21 items	23 items	18 items	13 items	22 items	9 items	16 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Input Capture	Fallback Channels		Network Denial of Service
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Man in the Browser	Multi-hop Proxy		Resource Hijacking
	InstallUtil	Component Firmware	Extra Window Memory Injection	Connection Proxy	Input Prompt	Process Discovery	Replication Through Removable Media	Screen Capture	Multi-Stage Channels		Runtime Data Manipulation
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Control Panel Items	Kerberoasting	Query Registry	Shared Webroot	Video Capture	Multiband Communication		Service Stop
	Local Job Scheduling	Create Account	Hooking	DCShadow	Keychain	Remote System Discovery	SSH Hijacking		Multilayer Encryption		Stored Data Manipulation
	LSASS Driver	DLL Search Order Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery	Taint Shared Content		Port Knocking		System Shutdown/Reboot
	Mshta	Dylib Hijacking	Launch Daemon	Disabling Security Tools	Network Sniffing	Software Discovery	Third-party Software		Remote Access Tools		Transmitted Data Manipulation
	PowerShell	Emond	New Service	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote File Copy		
	Regsvcs/Regasm	External Remote Services	Parent PID Spoofing	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Standard Application Layer Protocol		
	Regsvr32	File System Permissions Weakness	Path Interception	Execution Guardrails	Securityd Memory	System Network Connections Discovery			Standard Cryptographic Protocol		
	Rundll32	Hidden Files and Directories		Exploitation for Defense Evasion	Steal Web Session Cookie	System Owner/User Discovery					
	Scheduled Task	Hooking		Extra Window Memory Injection		System Service Discovery					
				File and Directory Permissions Modification		System Time Discovery					

MITRE ATT&CK® Navigator

__MapaLATAM | __GAP de Protección

selection controls | layer controls | technique controls

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	34 items	62 items	32 items	69 items	21 items	23 items	18 items	13 items	22 items	9 items	16 items
Spearphishing Link	Scripting	Registry Run Keys / Startup Folder	Scheduled Task	Scripting	Credentials in Files	File and Directory Discovery	Replication Through Removable Media	Screen Capture	Standard Cryptographic Protocol	Exfiltration Over Command and Control Channel	Resource Hijacking
Spearphishing Attachment	Scheduled Task	Scheduled Task	Process Injection	Deobfuscate/Decode Files or Information	Input Capture	System Information Discovery	Remote Desktop Protocol	Input Capture	Custom Cryptographic Protocol	Data Compressed	Stored Data Manipulation
Replication Through Removable Media	Rundll32	BITS Jobs	Bypass User Account Control	Masquerading	Credentials in Registry	Security Software Discovery	Remote File Copy	Clipboard Data	Custom Command and Control Protocol	Data Encrypted	Account Access Removal
Valid Accounts	PowerShell	Browser Extensions	New Service	Rundll32	Credentials from Web Browsers	Process Discovery	Exploitation of Remote Services	Data from Local System	Uncommonly Used Port	Automated Exfiltration	Data Destruction
Drive-by Compromise	Execution through API	Hidden Files and Directories	Valid Accounts	Disabling Security Tools	Credential Dumping	Application Window Discovery	Windows Admin Shares	Data from Removable Media	Standard Application Layer Protocol	Data Transfer Size Limits	Data Encrypted for Impact
Exploit Public-Facing Application	User Execution	New Service	Access Token Manipulation	Process Injection	Brute Force	Virtualization/Sandbox Evasion	AppleScript	Data Staged	Web Service	Exfiltration Over Alternative Protocol	Defacement
External Remote Services	Windows Management Instrumentation	Valid Accounts	Accessibility Features	Binary Padding	Network Sniffing	Peripheral Device Discovery	Application Deployment Software	Audio Capture	Commonly Used Port	Exfiltration Over Other Network Medium	Disk Content Wipe
Hardware Additions	Command-Line Interface	.bash_profile and .bashrc	AppCert DLLs	DLL Side-Loading	Account Manipulation	Remote System Discovery	Component Object Model and Distributed COM	Video Capture	Domain Generation Algorithms	Exfiltration Over Physical Medium	Disk Structure Wipe
Spearphishing via Service	Execution through Module Load	Accessibility Features	AppInit DLLs	File and Directory Permissions Modification	Bash History	System Network Configuration Discovery	Internal Spearphishing	Data from Network Shared Drive	Fallback Channels	Scheduled Transfer	Endpoint Denial of Service
Supply Chain Compromise	XSL Script Processing	Account Manipulation	Application Shimming	Virtualization/Sandbox Evasion	Exploitation for Credential Access	System Owner/User Discovery	Logon Scripts	Email Collection	Connection Proxy		Firmware Corruption
Trusted Relationship	Mshta	AppCert DLLs	DLL Search Order Hijacking	File Deletion	Forced Authentication	Network Share Discovery	Pass the Hash	Automated Collection	Data Encoding		Inhibit System Recovery
	AppleScript	AppInit DLLs	Dylib Hijacking	Modify Registry	Hooking	Network Sniffing	Pass the Ticket	Data from Information Repositories	Remote File Copy		Network Denial of Service
	CMSTP	Application Shimming	Elevated Execution with Prompt	Web Service	Input Prompt	Account Discovery	Remote Services	Man in the Browser	Communication Through Removable Media		Runtime Data Manipulation
	Compiled HTML File	Authentication Package	Emond	Obfuscated Files or Information	Kerberoasting	Browser Bookmark Discovery	Shared Webroot		Data Obfuscation		Service Stop
	Component Object Model and Distributed COM	Bootkit	Exploitation for Privilege Escalation	Software Packing	Keychain	Domain Trust Discovery	SSH Hijacking		Domain Fronting		System Shutdown/Reboot
	Control Panel Items	Change Default File Association	Extra Window Memory Injection	BITS Jobs	LLMNR/NBT-NS Poisoning and Relay	Network Service Scanning	Taint Shared Content		Multi-hop Proxy		Transmitted Data Manipulation
	Dynamic Data Exchange	Component Firmware	File System Permissions Weakness	Bypass User Account Control	Password Filter DLL	Password Policy Discovery	Third-party Software		Multi-Stage Channels		
	Exploitation for Client Execution	Component Object Model Hijacking	Hooking	Hidden Files and Directories	Private Keys	Permission Groups Discovery	Windows Remote Management		Multiband Communication		
	Graphical User Interface	Create Account	Image File Execution Options Injection	NTFS File Attributes	Securityd Memory	Query Registry			Multilayer Encryption		
	InstallUtil	DLL Search Order Hijacking	Launch Daemon	Process Hollowing	Steal Web Session Cookie	Software Discovery			Port Knocking		
	Launchctl	Dylib Hijacking	Parent PID Spoofing	XSL Script Processing	Two-Factor Authentication Interception	System Network Connections Discovery			Remote Access Tools		
	Local Job Scheduling	Emond	Path Interception	Code Signing		System Service Discovery			Standard Non-Application Layer Protocol		
	LSASS Driver	External Remote Services	Plist Modification	Connection Proxy		System Time Discovery					
	Regsvcs/Regasm	File System Permissions Weakness	Port Monitors	Indirect Command Execution							
	Regsvr32	Hooking	PowerShell Profile	Mshta							
	Service Execution	Hypervisor	Service Registry Permissions Weakness	Valid Accounts							
	Signed Binary Proxy Execution	Image File Execution Options Injection		Access Token Manipulation							
	Signed Script Proxy			Clear Command History							
				CMSTP							

La estrategia es más profunda y más simple

Enjoy safer technology!

ONLINE

INFOSECURITY SUMMIT

infosecurity MEXICO

En alianza con ISACA Mexico City Chapter ISACA Guadalajara Chapter

¡Gracias!

Miguel Ángel Mendoza
ESET Security Researcher
@angel_mendoza