CIBERAMENAZAS A LA SEGURIDAD PÚBLICA DEL 2021

ENFOQUE DEL PRODUCTO

Visión del Equipo de Inteligencia contra Amenazas de Motorola Solutions

MOTOROLA SOLUTIONS

D.A.ACOSTA
AGENTE
PFA

Como líder global en tecnología de seguridad pública, Motorola Solutions crea soluciones altamente innovadoras para la fuerza policial, bomberos, Servicios Médicos de Emergencia (SME), número 9-1-1 y otras agencias federales y estatales. Nuestro compromiso de entregar los mejores productos y servicios para el sector privado, con un enfoque en la ciberseguridad, nos proporciona una perspectiva directa de las ciberamenazas que retan específicamente al personal de primera respuesta en todo el mundo. Desde el 2018, el Equipo de Inteligencia contra Amenazas de Motorola Solutions ha compilado anualmente sus investigaciones y análisis para compartir directamente su visión con organizaciones de seguridad pública.

En 2021. conforme iniciamos el segundo año de la pandemia del COVID-19, el sector de seguridad pública (al igual que otros) se interconectó más, adquiriendo datos cada vez más integrados, después de tener sistemas dispersos. En el reporte anual de este año, compartimos nuestros hallazgos sobre cómo esta interconexión crea riesgos nuevos, exacerba los problemas conocidos y requiere niveles de vigilancia actualizados.

Para compilar este reporte, el Equipo de Inteligencia contra Amenazas utilizó datos privados y anónimos en conjunto con la información cibernética tanto privada como pública del 1 de enero al 15 de septiembre de 2021 en conjunto con una investigación integral del espacio tecnológico de la seguridad pública para identificar las amenazas más urgentes y significativas, los actores amenazantes y los riesgos en los servicios de emergencia.

El conocimiento es poder. Nos enfocamos en empoderar a los líderes y profesionales con la información que necesitan para minimizar el riesgo y adelantarse a los retos cibernéticos más significativos a lo largo del ecosistema esencial de la seguridad pública. Al compartir nuestra investigación, creemos que este reporte puede mejorar la seguridad y conciencia de las agencias y organizaciones enfocadas en tareas críticas que tienen la tarea de mantenernos a salvo.

ÍNDICE

RESUMEN EJECUTIVO 4
HERRAMIENTAS PARA LA SEGURIDAD PÚBLICA 5
RADIOS MÓVILES TERRESTRES 5
Sistemas del Proyecto Internacional 25 (P25) de APCO 6
Sistemas TETRA 6
Desarrollos de los Ciberataques en las Radios Móviles Terrestres 7
Mapeo de ATT&CK de MITRE 8
Acciones recomendadas 8
SUITE DE PUNTO DE RESPUESTA PARA LA SEGURIDAD PÚBLICA 9
El Punto de Respuesta de la Seguridad Pública 9
Manejo de llamadas 10
Despacho Asistido por Cómputo (CAD) 10
DESARROLLOS RECIENTES 11
Cambios en tipos de ataque 11
Actividad criminal en foros 12
Defensa recomendada 12
VIGILANCIA POR VIDEO 13
Video fijo 13
Estado actual de las cámaras y los nuevos riesgos de seguridad 13
Panorama de amenazas 14
Defensas actuales y recomendadas 15
LECTORES DE PLACAS VEHICULARES (LPR) 16
Dirección previa y riesgo de los datos y sistemas LPR 16
Cibercriminales 17
Hacktivistas 17
Estados nacionales 18
Vulnerabilidades comunes y métodos de infección 18
Panorama futuro de la industria de los LPR 18
ARMADO CON CONOCIMIENTO 19
GLOSARIO DE TÉRMINOS 20
FUENTES 21

RESUMEN EJECUTIVO

Identificar a actores amenazantes y sus técnicas profesionales nos ayuda a proporcionar recomendaciones más específicas para la seguridad.

Conforme el mundo sobrellevó el segundo año de la pandemia del COVID-19, nos hicimos más ágiles, adaptables e interconectados. Nuestras herramientas también lo hicieron. Estas herramientas nos permitieron ser productivos y eficientes sin importar dónde estábamos. Para la seguridad pública, esto significó contar con una respuesta a emergencias eficiente y confiable mientras combatía amenazas emergentes al alza contrarias a la disponibilidad, integridad y confidencialidad. Todo, desde radios, plataformas de comunicación, suites de despacho y hasta sistemas de vigilancia por video, tuvieron mayor vinculación, proporcionando un incremento en las capacidades simplificadas y de inteligencia. Sin embargo, los beneficios de estas herramientas de última generación también conllevan riesgos.

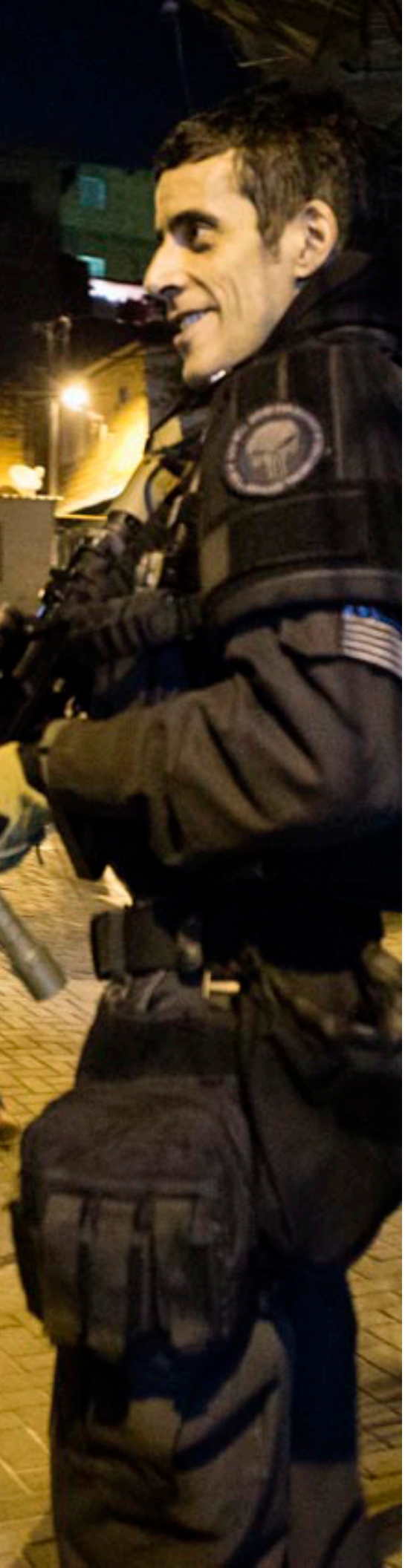
En el 2021, las amenazas de ciberseguridad se hicieron más sofisticadas, persistentes y amplias. Globalmente, las demandas de pago por rescate incrementaron en 82 por ciento, mientras que las consecuencias de los ataques de extorsión incrementaron debido a la adición de técnicas de robo de datos.1 Nuestro Equipo de Inteligencia contra Amenazas se enfocó en entender mejor las amenazas frecuentemente dirigidas a la seguridad pública. Identificar a actores maliciosos y sus técnicas profesionales nos ayuda a proporcionar recomendaciones de seguridad más específicas.

Los Puntos de Respuesta de la Seguridad Pública (PSAP), los cuales son críticos para enrutar las llamadas de emergencia, siguieron siendo los blancos más frecuentes, sufriendo más comúnmente de ataques de Negación del Servicio (TDoS) telefónicos de bajo impacto. Como resultado de siempre incrementar la conectividad con otros sistemas y dispositivos, las Radios Móviles Terrestres (LMR) sufrieron un ligero incremento en la cantidad de puestas en riesgo e incidentes de seguridad, incluyendo las infecciones por malware y ataques de ransomware. Las herramientas de vigilancia por video, tales como los lectores de placas vehiculares y cámaras de seguridad fijas, representan un blanco posible para actores relativamente poco sofisticados que podrían tratar de incrementar el tamaño de las botnets o hacer una declaración política mediante filtraciones de datos.

EL KIT DE HERRAMIENTAS DE SEGURIDAD PÚBLICA

RADIOS MÓVILES TERRESTRES

Las Radios Móviles Terrestres (LMR) permiten comunicaciones de “pulsar para llamar” de dos vías entre transceptores y pueden establecerse con muchas variaciones diferentes, incluyendo las portátiles y montadas en vehículos o bases fijas. Se utilizan en varias industrias, incluyendo las comunicaciones esenciales de seguridad pública y comunicaciones privadas en industrias comerciales, tales como las del sector petrolero. Ya que las LMR proporcionan comunicaciones instantáneas y seguras, a menudo son el método de comunicación principal en estas industrias, particularmente en ambientes en donde el servicio de telefonía celular es impráctico debido a que no existe o tiene cobertura limitada.



SISTEMAS DEL PROYECTO INTERNACIONAL 25 (P25) DE APCO

Los sistemas tradicionales o de enclave P25 LMR no se aíslan completamente de la internet y no deberían considerarse como inherentemente seguros. Si bien lo más común es que operen detrás de dos firewalls, tenemos una creencia moderada de que la topografía de red de los sistemas de enclave y las cuentas con privilegios altos podrían de todos modos permitir que un atacante paciente o empedernido lograse acceso en raras ocasiones. Esta valoración se basa en los modelos de red disponibles y en las configuraciones de despliegue conocidas.

Las configuraciones erróneas y el no aprovechar las características de seguridad disponibles en su totalidad son los obstáculos más comunes en los sistemas LMR de P25. Utilizar cuentas administrativas integradas en vez de cuentas sin privilegios para el uso habitual y contar con políticas de firewall ausentes o mal configuradas para segmentar la red de LMR desde redes adyacentes son las malas configuraciones que se reportan con mayor frecuencia para los sistemas P25. Sin embargo, en algunas instancias, los sistemas P25 que se configuraron correctamente no estaban aprovechando todas las características de seguridad disponibles y nativas para sus sistemas tales como los Sistemas de Prevención de Intrusiones (IPS) en los hosts, lo cual hizo imposible que se detectara a los atacantes. Exhortamos a todos los usuarios de sistemas P25 a trabajar junto con sus proveedores para asegurarse de que entienden y aplican tantas capacidades de seguridad nativas disponibles como sea posible.

Tomar ventaja de las vulnerabilidades en soluciones de acceso remoto puede permitir el acceso a, o controlar, un ambiente central de P25. Desde el principio de la pandemia del Covid-19, la comunidad de ciberseguridad global ha visto un esfuerzo concentrado de actores malintencionadas para encontrar y aprovechar las vulnerabilidades en las soluciones de acceso remoto, tales como las VPN. Si bien no es exclusivo de los sistemas P25, las soluciones de VPN de Palo Alto, Fortinet y Pulse Secure son ejemplos que reportó la CISA en el 2020 y 2021 debido a sus vulnerabilidades que permitieron a actores malintencionados tomar ventaja. Las VPN no son intrínsecamente inseguras. Sin embargo, cuando las vulnerabilidades se dan a conocer, debe priorizarse aplicar las mitigaciones recomendadas y, siempre que sea posible, utilizar la autenticación multifactorial para sus cuentas.

SISTEMAS TETRA

Cuando se compara con los sistemas P25, TETRA tiene problemas de seguridad diferentes. Con base en las observaciones, los sistemas TETRA permiten conexiones remotas en instancias poco comunes.

Existe un potencial de los administradores TETRA que ejecutan conexiones desde fuera de sus redes de TI, mediante firewall, hacia los sistemas TETRA. Estas conexiones se administran frecuentemente mediante soluciones de acceso remoto de terceros.

Tanto en los casos de ambientes APCO P25 y TETRA, es factible que las vulnerabilidades de las soluciones de acceso remoto o firewall puedan permitir que un atacante abuse estas conexiones remotas.

Para mitigar este problema, los usuarios deberían consistentemente seguir mejores prácticas, tales como la aplicación frecuente de parches y auditorías, rotación de credenciales de acceso y la inhabilitación de puertos y servicios sin utilizar.

DESARROLLOS DE CIBERATAQUES EN RADIOS MÓVILES TERRESTRES

La última vez que realizamos una revisión integral del panorama de amenazas a las LMR fue a mediados del 2020. Desde entonces, el cambio más significativo en los ataques a los sistemas LMR ha sido un incremento mínimo en la Negación de Servicios de Transmisión (BDoS) y otro en los datos cifrados para impactar a los sistemas de las LMR. Los ataques de BDoS ocurrieron en conjunto con disturbios sociales más amplios, específicamente cuando los gobiernos locales promulgaron toques de queda y se estaban suscitando protestas ciudadanas, especialmente durante el verano del 2020. Es altamente probable que dichos ataques de BDoS se llevaran a cabo como consecuencia directa de las protestas más amplias y que tuvieran motivaciones ideológicas. Los ataques de ransomware que impactan a las LRM muy seguramente tuvieron un interés financiero y parecían tomar ventaja de las malas configuraciones y contraseñas predeterminadas. Tanto los ataques de BDoS como los de ransomware colocaron a la negación de servicios (DoA) como el impacto más alto de los ataques, siendo cuatro de cada cinco incidentes un ataque de DoA. Por lo tanto, evaluamos con confianza moderada que cualquier ataque exitoso con motivación ideológica o financiera a las LMR muy probablemente dará como resultado un impacto en la disponibilidad de dichos sistemas, ya sea mediante la interrupción de las comunicaciones aéreas o al cifrar los servidores de administración de radios.

Observamos anteriormente a criminales no técnicamente sofisticados utilizar el robo de llaves o hardware como forma de obtener acceso a las comunicaciones cifradas de la fuerza policial y crear sus propios canales privados. Esta tendencia ha continuado desde mediados del 2020. El 22 de junio de 2020 el Departamento de Policía de Toronto anunció que sus investigaciones descubrieron un plan para proporcionar radios policiales robadas a los conductores de las grúas de la ciudad y se acusó de ello a 11 individuos. La operación criminal colocó a los dispositivos policiales cifrados en manos de varios choferes que trabajaban para varias organizaciones de grúas en Toronto.

Estos choferes planeaban utilizar las radios para vigilar las comunicaciones policiales, tomando así ventaja para encontrar y llegar a las escenas de accidentes vehiculares antes que la competencia. Este "sistema de notificación temprana" estuvo disponible especialmente para los conductores de camiones durante el punto más alto del encierro por pandemia del COVID-19 en Toronto, ya que, al haber menos conductores en el camino, lo cual redujo la cantidad total de accidentes. Los investigadores confiscaron tres radios, seis grúas y un arma como parte de estos arrestos. La policía de Toronto arrestó por lo menos a un oficial que estaba conectado con los robos de las radios.2 Con base en la prevalencia de la táctica de robo de llaves o hardware en riesgos sencillos, estimamos con mucha confianza que este método seguirá siendo popular, especialmente entre los individuos o grupos que buscan ya sea evadir o monitorear a las fuerzas policíacas.

Durante la respuesta a incidentes y la investigación de los ataques a los sistemas de LMR, el Equipo de Inteligencia contra Amenazas de Motorola Solutions pudo identificar las técnicas profesionales que más utilizaron los atacantes, las cuales incluyen el escaneo de bloques IP del sistema objetivo, así como el escaneo de vulnerabilidades como parte de sus esfuerzos de reconocimiento inicial. En instancias como el ejemplo anterior de Toronto, las personas malintencionadas a menudo dependían de un "acceso inherente", utilizando a los internos para que les proporcionaran radios o llaves de cifrado robadas. Mientras tanto, los actores amenazantes menos sofisticados utilizaron métodos de acceso tradicional, tales como poner en riesgo los servicios remotos y aprovechar las aplicaciones de contacto con el público para intervenir en las redes vulnerables y expuestas de LMR y en los sistemas adyacentes. Una vez dentro de las redes objetivo, se observó que los atacantes obtuvieron cuentas de dominio predeterminadas para conseguir privilegios elevados.

Se identificó a los atacantes retirando indicadores de los hosts durante un ataque para evitar la detección y atribución. En todas las instancias observadas, investigadas o valoradas de riesgos a las LMR, los atacantes ya sea condujeron un ataque de BDoS o ejecutaron ransomware para cifrar datos cuando no buscaban vigilar las comunicaciones de la fuerza policial ni establecer su propio canal clandestino.

Es factible que las vulnerabilidades en ese firewall o las soluciones de acceso remoto pudieran permitir que un atacante abusara de tales conexiones remotas. Para mitigar este problema, los usuarios deberían consistentemente seguir mejores prácticas, tales como los parches frecuentes y el inhabilitar los puertos y servicios que no utilizan.

MAPEO DE LAS LMR DE ATT&CK DE MITRE

RECONOCIMIENTO	ACCESO INICIAL	EJECUCIÓN	PERSISTENCIA	ESCALAMIENTO DE PRIVILEGIOS	EVASIÓN DE DEFENSAS
Escanear los bloques de IP	Robo de llaves/hardware	PowerShell	Servicios Remotos Externos	Saltarse el Control de Cuentas de Usuario	Eliminación de indicadores en el host
Escaneo de vulnerabilidades	Acceso inherente (amenaza interna)	Shell de Comandos de Windows	Crear o modificar el proceso de Windows	Inyección del proceso	Inhabilitar o modificar a las herramientas
	Replicación mediante medios eliminables	Shell de Unix		Aprovechamiento del escalamiento de privilegios	Inhabilitar el registro de eventos de Windows
	Servicios Remotos Externos	Instrumentación de la administración de Windows (WMI)			Archivos o información ofuscada
	Aprovecharse de la aplicación de contacto al público	Ejecución de Servicios			Coincidencia legítima Nombre o ubicación
	Cuentas predeterminadas	API Nativas			Modificar el registro
	Cuentas de dominio	Python			Ejecución errónea firmada
	Poner en riesgo las dependencias de gobierno y laves de desarrollo				Ejecución Regsvr32 firmada
	Comprometer la cadena de suministro de software				Ejecución Rundll32 firmada

ACCESO A LAS CREDENCIALES	DESCUBRIMIENTO	MOVIMIENTO LATERAL	RECOLECCIÓN	COMANDO Y CONTROL	EXFILTRACIÓN	IMPACTO
Rociado de contraseñas	Descubrimiento de procesos	Transferencia lateral de herramientas	Captura de audio	Canal cifrado	Exfiltración por canal C2	Negación de Servicio de Transmisión (BDoS)
Suplantación de credenciales	Escaneo de servicios de red	Replicación mediante medios eliminables	Datos de sistemas locales	Proxy externo	Exfiltración por protoeolo simétrico cifrado diferente al C2	Datos cifrados para el impacto
Adivinar contraseñas	Descubrimiento de información del sistema	Servicios remotos (en caso de ser aplicable)	Datos del repositorio de configuraciones	Puerto no estándar	Extracción por protocolo cifrado asimétrico diferente al C2	Apagado/reinicio del sistema
Volcado del sistema de credenciales del SO	Descubrimiento de los servicios del sistema				Exfiltración por protocelo no cifrado/no ofuscado diferente al C2	Destrucción de datos
Credenciales en los archivos	Descubrimiento de grupos de dominio					Secuestro de recursos
	Descubrimiento de las conexiones de la red del sistema					Detención de servicios
	Compartir la red					Inhibir la recuperación del sistema
	Descubrimiento de archivos y directorio					Negación del servicio en redes
	Reconocimiento de red					

LEYENDA
Probable
Probable
Posible
Poco probable/raro

ACCIONES RECOMENDADAS

La naturaleza de cada vez mayor conexión en los sistemas LMR no empata bien con el alza de atacantes sofisticados. Esta combinación requiere que los operadores y técnicos de LMR garanticen un enfoque de seguridad integral, requerido y por capas. También requiere que los usuarios de LMR aseguren que esos controles de seguridad nativos se implementen en el momento de la instalación, durante la operación y se complementen con los controles administrativos, políticas y procedimientos.

La autenticación multifactorial debe habilitarse y requerirse para todas las cuentas disponibles que accedan a la DMX y al núcleo de un sistema de LMR. Los dispositivos cuyo acceso se haya comprometido pueden introducir diversas amenazas a los ambientes de LMR en la nube, de acuerdo con lo que define el Instituto Nacional de Estándares y Tecnología en su catálogo de amenazas móviles.[3]

Finalmente, los procedimientos para reportar el equipo perdido o robado, auditorías frecuentes de inventario del equipo de radio, así como para inhabilitar dicho equipo, deben implementarse siempre que sea posible. Esto puede ayudar a identificar cuando las Tácticas, Técnicas y Procedimientos (TTP) de robo de llaves o hardware pueden ser usadas por actores internos o atacantes poco sofisticados.

SUITE DE PUNTO DE RESPUESTA PARA LA SEGURIDAD PÚBLICA

EL PUNTO DE RESPUESTA DE LA SEGURIDAD PÚBLICA

Los Puntos de Respuesta de Seguridad Pública (PSAP, por sus siglas en inglés) son centros que procesan llamadas de emergencia. Habitualmente, tienen cinco flujos de comunicación principal: llamadas entrantes al número 9-1-1, tráfico de SMS entrante, consultas de ubicación salientes, tráfico de despacho saliente y líneas administrativas bidireccionales. Esta infraestructura crítica habilita al personal de respuesta a emergencias para que esté informado y responda a eventos relevantes que afectan al público. Con la implementación de los servicios de red telefónica basados en IP y la tecnología en evolución, los PSAP deben prepararse para administrar activamente posibles amenazas de ciberseguridad, incluyendo los ataques de Negación de Servicio Telefónico (TDoS), ransomware y otros tipos de accesos no autorizados a datos y sistemas. Con el aumento en el uso de las plataformas basadas en IP y el incremento correspondiente de la superficie de ataque que los acompaña, el riesgo de los ataques de seguridad y otras amenazas contra los PSAP probablemente tenderán a crecer.

MANEJO DE LLAMADAS

El manejo de llamadas se logra mediante software basado en telefonía y en IP, el cual se utiliza para aceptar, poner en la fila y responder llamadas de emergencia. Los sistemas de manejo de llamadas de la generación actual también pueden aceptar mensajería basada en SMS. Hacia el futuro se espera que estas soluciones procesen otros tipos de tráfico de mensajería de emergencia, tal como la multimedia.

Una de las amenazas más significativas a los PSAP es el ataque de TDoS a través de líneas telefónicas físicas y basadas en IP.4 Los autores de las amenazas aprovechan los ataques de TDoS contra las líneas telefónicas administrativas y del número 9-1-1, las cuales pueden dar como resultado una interrupción en la capacidad de manejo de las llamadas. Si bien estos ataques a menudo no se reportan, siguen siendo el tipo más común de ellos que hemos observado que involucran a los PSAP. Estos ataques son extremadamente fáciles de llevar a cabo, ya que requieren un grado bajo o nulo de pericia.

Un atacante puede llevar a cabo un TDoS de dos formas: manual y automatizada. Para el caso de los ataques de TDoS manuales, los autores de la amenaza pueden acceder a una cantidad arbitraria, pero a menudo grande, de teléfonos. Estos pueden ser teléfonos desechables de prepago o teléfonos puestos en riesgo con malware. En cualquiera de los casos, el atacante puede aprovechar estos dispositivos haciéndolos marcar a números de emergencia, sobrecargando los PSAP con llamadas generadas manualmente.
Los ataques automatizados son más fáciles de llevar a cabo. Solo necesitan acceso a un sistema de telefonía virtual capaz de desplegar una gran cantidad de llamadas generadas por computadora.

Esto se puede lograr si rentan el acceso a botnets de bajo costo o incluso si ejecutan programas simples a través de computadoras u otras estaciones de trabajo.
La motivación detrás de los ataques de TDoS van desde lo ideológico hasta lo financiero o incluso adquirir notoriedad. Sin embargo, los reportes disponibles de víctimas sugieren que es posible que los atacantes con poca pericia busquen principalmente obtener dinero con planes de TDoS al extorsionar los PSAP por recompensas de rescate. Estos atacantes de TDoS con un interés financiero a menudo no están afiliados con grupos específicos y deciden actuar por sí solos.

Los sistemas 9-1-1 de Última Generación (NG9-1-1) son más resilientes a los ataques de TDoS que los sistemas tradicionales, ya que pueden manejar una cantidad mucho mayor de llamadas simultáneas que los sistemas más viejos. Sin embargo, los ataques de TDoS siguen siendo un problema para los NG9-1-1. Si bien los sistemas de NG9-1-1 pueden soportar las llamadas masivas que despliegan los atacantes de TDoS, los empleados de los PSAP en el extremo receptor de estas llamadas no tienen tanta suerte.

En los sistemas más viejos, diferentes a los NG9-1-1, los ataques de TDoS impactaron las líneas telefónicas de los proveedores de servicios debido a que la carga de llamadas era mayor al ancho de banda de la telefonía. En los NG9-1-1, estas llamadas fraudulentas obtienen acceso, lo cual da como resultado que los receptores tengan que contestarlas. Las llamadas "reales" se mezclan con estas falsas conforme los ciudadanos intentan contactar a los servicios de emergencia. Esto da como resultado que las personas tengan que esperar más para que se respondan sus llamadas, lo cual a menudo conlleva que las llamadas se abandonen o se tenga que volver a marcar y esto crea otro TDoS efectivamente dentro del ataque original.

Cuando se conducen los ataques de TDoS contra los PSAP, los actores que originan las amenazas podrían posicionar las llamadas durante los momentos en donde los defensores no pueden responder proactivamente debido al alto volumen de llamadas o a poco personal. Protestas generalizadas o desastres naturales como los incendios forestales podrían dar como resultado una gran cantidad de llamadas legítimas al 9-1-1. Mientras tanto, horarios después de la jornada laboral y algunos días festivos podrían resultar en menos personal de despacho trabajando. Cualquiera de estas situaciones empeorará los efectos perjudiciales de los ataques de TDoS.

DESPACHO ASISTIDO POR CÓMPUTO (CAD)

Los despachadores, telefonistas y operadores del 9-1-1 aprovechan los sistemas de Despacho Asistido por Cómputo (CAD) para enviar al personal de emergencia a donde se le necesita más. Los despachadores también utilizan los sistemas CAD para identificar la ubicación y el estado del personal de primera respuesta, adicionalmente a priorizar y grabar las llamadas de emergencia entrantes.

El ransomware es la amenaza más común a los sistemas CAD, lo cual los impacta de dos formas. La primera es a través de los ataques indirectos a redes policiales y municipales. Estos ambientes policiales y municipales a menudo funcionan como la columna vertebral de las redes para los sistemas CAD. En caso de que haya un ataque de ransomware, los defensores podrían inhabilitar los servicios de red como precaución, como parte de la respuesta a incidentes, o durante las actividades posteriores de restablecimiento de datos. Cada uno de estos escenarios podrían dar como resultado interrupciones en los servicios CAD.
La segunda forma en la que el ransomware puede impactar a los sistemas CAD es al comprometer directamente las mismas redes CAD. Un ataque que comprometa directamente es menos frecuente, pero sí llega a ocurrir, especialmente cuando se exacerba debido a malas configuraciones o servicios poco seguros. Los riesgos directos de las redes CAD a menudo vienen de conexiones confiables entre el ambiente CAD y las redes policiales o municipales adyacentes. Estas también ocurren cuando las estaciones de trabajo CAD se habilitan con una conectividad de salida al internet, una práctica que no es estándar y no se recomienda. Finalmente, los servicios entrantes tales como las conexiones VPN pueden ponerse en riesgo en instancias poco comunes, llevando a que los autores de las amenazas accedan a los sistemas CAD desde el internet abierto u otras redes.

DESARROLLOS RECIENTES

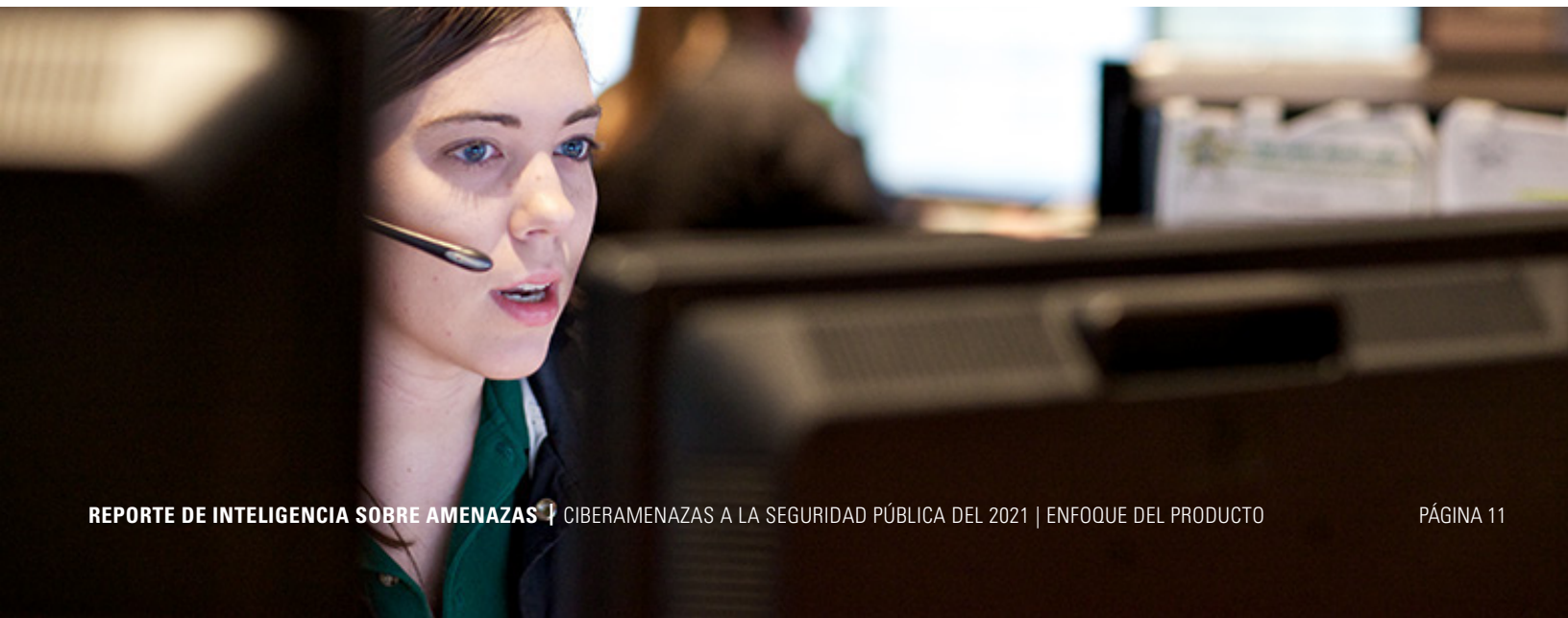
CAMBIOS EN TIPOS DE ATAQUE

La última vez que realizamos una revisión integral del panorama de amenazas a los PSAP fue en agosto del 2020. Desde entonces, los ataques a los PSAP aumentaron. Hubo un 38 por ciento de alza en los ataques reportados en la segunda mitad del 2020 y el inicio del 2021. Esto fue, en su mayoría, debido a cinco ataques de TDoS en contra de los centros de despacho en los Estados Unidos, lo cual dio como resultado una degradación de los servicios de manejo y toma de llamadas en cada instancia. En el periodo de reporte anterior, no se reportaron ataques de TDoS. Sin embargo, estos eventos no se divulgan frecuentemente y, por lo tanto, se puede declarar con mucha confianza que es posible que los ataques de TDoS hayan ocurrido sin haberse registrado. Una notificación de valoración de amenazas estatales que se publicó en mayo del 2021 denotó un "amplio incremento en los ataques de negación de servicio telefónico" a los PSAP en toda la nación. Con base en este análisis, el incremento que se observó en los ataques de TDoS desde el 1 de agosto de 2020 podría indicar que ya sea ocurren más de estos eventos o que se están reportando más. En este momento no se puede determinar con confianza cuál es la verdadera razón.

Hubo una baja del 42 por ciento en los ataques de ransomware que impactan a los PSAP y solo se reportaron cuatro desde el 1 de agosto de 2020. Esta baja en los ataques observados de ransomware contra los PSAP no tiene una sola causa. Sin embargo, se le puede atribuir parcialmente al incremento en la preparación de las municipalidades de los Estados Unidos contra este tipo de ataques. Adicionalmente, las comunicaciones de las organizaciones como la Agencia de Seguridad en Infraestructura y Ciberseguridad impulsaron la implementación de mejores prácticas, tales como respaldar información fuera de línea. Probablemente esto ocasionó menos casos de encriptación de redes municipales y respaldos dedicados. Como tal, se evalúa que el impacto a las redes PSAP conectadas disminuyó debido a que hubo menos casos en que cayeran redes municipales principales o estas fueran inhabilitadas durante acciones de respuesta a incidentes de la ciudad.

Solo hubo un incidente en donde se identificó el malware detrás de un ataque de ransomware con cualquier tipo de seguridad. El 24 de junio de 2021, un atacante no identificado tuvo éxito en poner en riesgo un centro de despacho en el sur de Estados Unidos. Los defensores respondieron inhabilitando dos máquinas virtuales y un servicio de Red Privada Virtual (VPN) a la cual había accedido el atacante. Los archivos se sufijaron con una extensión ".eight" durante el ataque. Creemos que el atacante utilizó una variante del ransomware Phobos y, por lo tanto, pudo haber estado afiliado o ser un cliente de dicha operación de ransomware. Esta evaluación se basa en el hecho de que la nota de la solicitud de rescate de la apelación ".eight" comparte similitudes con las de Phobos y se utiliza como una extensión de archivo de este. La variante de malware ".eight" se distribuye más a menudo a través de los correos electrónicos de phishing con archivos adjuntos maliciosos, sitios de torrent no seguros y sitios malintencionados.

Los ataques físicos que no dependen de las capacidades cibernéticas permanecieron sin cambios durante el periodo de este reporte y se identificó a uno en el periodo anterior y uno que se suscitó el 25 de diciembre de 2020. El último consistió en que el terrorista, Anthony Quinn Warner, detonó un explosivo en su camioneta junto a un concentrador de redes de AT&T en Tennessee, suicidándose y lastimando a otras tres personas. La explosión causó una interrupción amplia de las comunicaciones en todo el estado. Los servicios de telefonía celular, alámbrica y de internet se vieron afectados, así como diversas redes locales de 9-1-1 y diferentes a las de emergencia en la región. Es muy poco probable que cualquier tipo de ataque físico contra los PSAP provenga de una motivación de ganancias financieras y que, en vez de esto, se cimiente en las motivaciones individuales, terroristas o de grupos ideológicos.



ACTIVIDAD CRIMINAL EN FOROS EN INTERNET

La confiabilidad de los ataques de TDoS se desarrolló debido a la prevalencia de la tecnología "Voz sobre IP" (VoIP), lo cual permite que los individuos envíen una cantidad arbitraria de "llamadas telefónicas" sin primero tener que obtener acceso a una matriz más grande de teléfonos.

El Equipo de Inteligencia contra Amenazas de Motorola Solutions notó a individuos que ofrecen servicios que podrían utilizarse en los ataques de TDoS (Véase la imagen 10). Tal como se mencionó anteriormente, estos ataques se llevan a cabo de forma virtual. Esta es una evolución del método predeterminado de utilizar a un host de teléfonos infectados para llamar al 9-1-1, lo cual fue el caso en el ataque manual de TDoS del 2016 que organizó un adolescente de Arizona.[6] La confiabilidad de los ataques virtuales de TDoS se desarrolló debido a la prevalencia de una tecnología de "Voz sobre IP" (VoIP), la cual permite que las personas envíen una cantidad arbitraria de "llamadas telefónicas" sin primero tener que obtener acceso a una matriz más amplia de teléfonos. Evaluamos previamente que estos ataques virtuales de TDoS se originaron de una actividad de botnet, específicamente de máquinas con capacidades de VoIP en la "dark web" o en foros con actividad criminal.

Hubo varios miembros que se observaron vendiendo servicios de "saturación telefónica" en foros clandestinos, con precios tan bajos como $3 dólares por hora. Estos servicios de saturación incluían llamadas telefónicas virtuales y capacidades de saturación por SMS que un usuario describió como un ataque de negación de servicio distribuido (DDoS) para teléfonos. Si bien no hubo instancias de objetivos de seguridad pública o tecnologías que se hayan mencionado asociadas con estos servicios de saturación, estamos convencidos de que estos recursos pueden utilizarse contra los PSAP; específicamente, contra los sistemas de manejo y toma de llamadas. Es probable que muchos individuos o grupos detrás de los ataques de TDoS utilicen servicios de saturación de llamadas como estos.

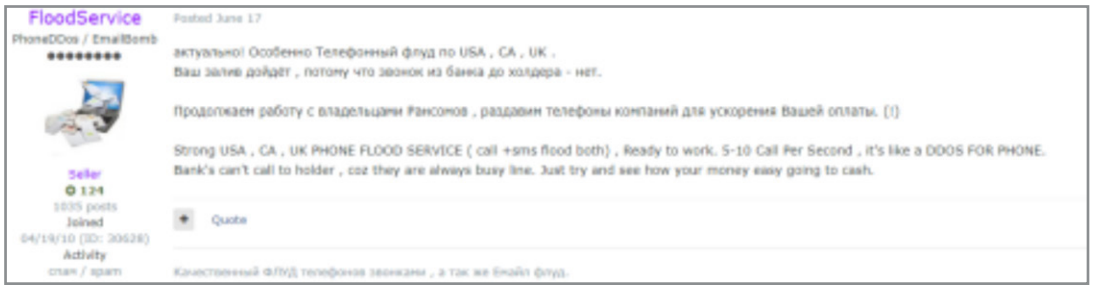


Figura 10: Un usuario de un foro clandestino, "Floodservice", vendiendo servicios de saturación de llamadas y SMS.

DEFENSAS RECOMENDADAS

La naturaleza interconectada de los PSAP, tanto con los servicios de toma/manejo de llamadas como con las redes CAD, requieren que los diseñadores de los productos implementen un enfoque de seguridad integral y requerido por capas. Las VPN entrantes; conexiones a redes municipales y adyacentes; las cuentas de dominio de uso amplio y las estaciones de trabajo ocasionalmente habilitadas para conectarse a la internet representan riesgos de seguridad potenciales que podrían facilitar un ataque en contra de los sistemas CAD dentro de los PSAP. Mientras tanto, no puede existir una defensa confiable contra los ataques de TDoS. El crear opciones de respaldo para cuando se interrumpen las llamadas de emergencia o al 9-1-1 puede ayudar a proporcionar una oportunidad para que los ciudadanos aún puedan interactuar con los administradores de las llamadas durante alguna emergencia. El publicar líneas telefónicas diferentes a las de emergencia en los sitios de redes sociales ha, por lo tanto, sido por mucho la táctica más común que utilizan los defensores mientras están a mitad de un ataque de TDoS. Sin embargo, estas líneas telefónicas también pueden ser el objetivo de los atacantes de TDoS, por lo que enrutar llamadas a condados cercanos sigue siendo una práctica común.

Implementar la MFA, cuando es adecuada y aplicable, puede servir para limitar el peligro de contar con credenciales VPN puestas en riesgo. Las órdenes ejecutivas recientes en los Estados Unidos impulsaron la modernización e implementación de estándares de ciberseguridad más resistentes mediante una arquitectura de confianza cero. Dichas órdenes incluyeron un mandato para utilizar MFA para garantizar que los sistemas federales se protejan contra las amenazas de ransomware que están creciendo. Cualquier tolerancia hacia estaciones de trabajo conectadas al internet dentro de las redes PSAP deberían documentarse, ya que las estaciones de trabajo conectadas a internet representan un riesgo y son un vector probable para las infecciones por ransomware. Por último, tal como se mencionó anteriormente, una de las interrupciones más comunes a los PSAP sucede cuando una red municipal adyacente o "pilar" se inhabilita como resultado de una infección por ransomware. En estos casos, incluso cuando la misma red del PSAP no se pone en riesgo directamente, puede suscitarse una degradación de los servicios o incluso una ausencia de los mismos. Como tal, los centros de despacho deben esperar que los ataques de extorsión en las redes municipales tengan una oportunidad significativa para impactar también las funciones de manejo/recepción de llamadas de 9-1-1 o de CAD.

VIGILANCIA POR VIDEO

VIDEO FIJO

ESTADO ACTUAL DE LAS CÁMARAS Y LOS NUEVOS RIESGOS DE SEGURIDAD

El desarrollo de las nuevas tecnologías de video fijo permite el monitoreo sofisticado y la alerta de actividad malintencionada irregular en los ambientes físicos. Para lograr una vigilancia por video de última generación, las soluciones de video fijas se migraron de cámaras de video análogas a cámaras basadas en IP. Esto crea un vector de amenazas significativo y nuevo que incrementa el área de amenazas para sistemas anteriormente aislados.

Es poco probable que muchos de los clientes de las soluciones de video fijas puedan entender el incremento de las amenazas como un resultado de esta transición. Esto da como resultado que muchos de los sistemas de vigilancia fija no se parchen, monitoreen o aseguren.
Del millón de cámaras y de los 125,000 servidores expuestos que identificó Shodan, el 90 por ciento se expusieron a través de HTTP, 8 por ciento a través de telnet, 8 por ciento a través de SSH y 3 por ciento a través de MySQL. Es posible que estos tipos de exposición permitieran que los atacantes obtuvieran acceso a las redes de vigilancia, facilitando las operaciones criminales debido a las vulnerabilidades conocidas, sin parchar o por descubrir en los protocolos o en los mismos productos.[7]

Otros sistemas de cámaras nuevos y basados en IP se están integrando en las ofertas de servicios en la nube, lo cual permite el acceso, visualización y control remoto de las redes de cámaras. El acceso adicional a los servicios en la nube incrementa la oportunidad de las malas configuraciones o de las cuentas y llaves expuestas que podrían permitir a los atacantes obtener acceso a todos los juegos de redes de cámaras o a aquellas individuales. Por ejemplo, el 9 de marzo del 2021, el colectivo de hackers "APT69420", al cual también se le hace referencia en fuentes públicas como "Arson Cats", descubrieron credenciales expuestas en el código para una cuenta de súper administrador de Verkada en la infraestructura de DevOps expuesta al internet.

Cualquier y todo ambiente de DevOps expuesto a la internet podría dar como resultado una falla de seguridad crítica que los atacantes podrían tomar como objetivo para sus labores de reconocimiento, ya que más frecuentemente, las credenciales y llaves de acceso sensibles se exponen en el código como resultado de las prácticas inseguras. Las auditorías adecuadas y frecuentes, así como las políticas de seguridad requeridas, son esenciales para desarrollar equipos para inhibir cualquier exposición accidental. En el incidente de Verkada, las cuentas de "súper administrador" expuestas en el código del ambiente DevOps permitieron que los atacantes vieran todas las grabaciones de vigilancia de los clientes que respaldaba el servicio en la nube.[8]

PANORAMA DE AMENAZAS

Estamos casi seguros que los atacantes que pudieran comprometer los sistemas de video vigilancia fijos no son muy sofisticados. Esto incluye a los hacktivistas con motivaciones ideológicas, botnets con motivación financiera u operadores de criptominería y "script-kiddies" que quieren ganar notoriedad.9 Basamos esta evaluación en los TTP que utilizaron los atacantes en los escenarios de riesgo observados, así como en la poca prevalencia de los datos valiosos en los sistemas de video fijo cuando se comparan con otras tecnologías de seguridad pública.

Es poco probable, pero posible, que las redes de cámaras IP también puedan ser un objetivo de los atacantes más sofisticados para facilitar la actividad criminal o de espionaje en las redes empresariales adyacentes, pero seguramente requerirían despliegues de sistema mal configurados y conectados a redes empresariales adyacentes o abiertos a la internet. Los sistemas de video fijo se evalúan con una confianza moderada para representar un valor financiero mínimo para atacantes sofisticados.

Los sistemas de video fijo se despliegan a menudo en escuelas, estadios, ubicaciones manufactureras y sitios gubernamentales. Los datos que almacenan estos sistemas suelen ser poco vitales para las organizaciones en sus funciones diarias. Por lo tanto, es poco probable que el video fijo sea un objetivo principal de los famosos grupos criminales electrónicos. De la misma forma, es raro que los datos de video fijo contengan información valiosa y esta no representa un objetivo probable de las campañas de espionaje. Como tal, no se ha observado ni identificado a ningún grupo de amenaza prominente o que se sepa sea sofisticado, el cual tenga como objetivo algún sistema de video fijo. Sin embargo, ya que mantener y proteger la privacidad de aquellos a los que se monitorea, tal como en el caso de las escuelas, el proteger los activos de seguridad en video es esencial para garantizar que las fuentes de video no se expongan.

La amenaza más frecuente contra los sistemas de vigilancia por video es la absorción en botnets, lo cual da como resultado una posible degradación del servicio. El 12 de octubre de 2016, la botnet Mirai escaneó la internet abierta en búsqueda de puertos Telnet.[10]

Entonces, esta botnet aprovechó una combinación de 61 combinaciones de usuario/contraseña que se utilizan frecuentemente como credenciales predeterminadas en dispositivos del internet de las cosas (IoT) para intentar ingresar en sistemas identificados. En estos sistemas del IoT se incluyeron cámaras de video por IP fijas. Después de infectar las cámaras IP y otros dispositivos del IoT, la botnet Mirai lanzó un ataque de negación de servicio distribuido (DDoS) a gran escala contra la infraestructura de DNS de la organización Dyn, interrumpiendo sus servicios de internet para la costa este de los Estados Unidos. En la cúspide de la botnet, hubo aproximadamente 600,000 instancias simultáneas de dispositivos del IoT infectados.[11]

Desde el 2016, la botnet IRCTelnet puso en riesgo cámaras IP a través de Telnet mediante intentos de ataque de fuerza bruta y credenciales predeterminadas de la misma forma que Mirai, aunque con un alcance menor.[12] Las botnets toman como objetivo los dispositivos del IoT para incorporarlos en ataques de DDoS como Mirai, pero también para hacer minería de criptodivisas. Otros individuos han mostrado interés para obtener acceso al video fijo y en los sistemas Aviglion, (véase la Imagen A a continuación). Esto puede facilitar un comportamiento de seguimiento, tal como crear o aumentar una botnet y exponer datos de video, pero también permitir actividades de extorsión en algunos casos. El comportamiento anterior se representa con los siguientes TTP: servicios remotos, cuentas predeterminadas, adivinar contraseñas, secuestro de recursos y negación de servicios en redes.[13]

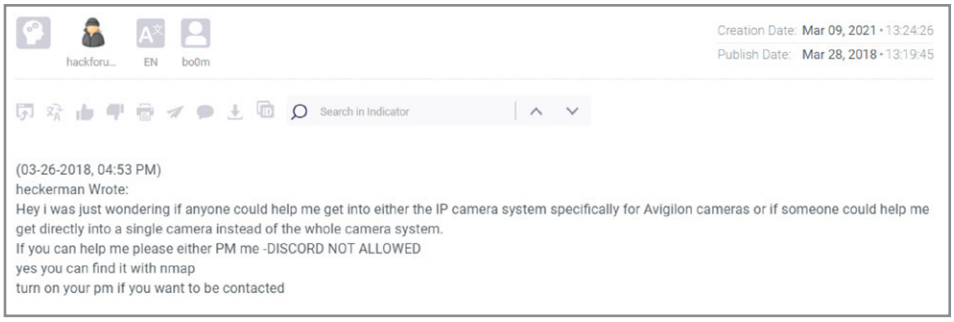


IMAGEN A: El usuario "heckerman" preguntando sobre cómo obtener acceso al sistema de cámaras IP de Avigilon.

El 9 de marzo de 2021, se reportó que los atacantes obtuvieron acceso a la compañía de cámaras de vigilancia Verkada, y también a 150,000 cámaras instaladas en toda su base de clientes. Supuestamente, los atacantes obtuvieron acceso a estos sistemas utilizando una cuenta de súper administrador de Verkada que descubrieron en la infraestructura de DevOps, la cual se expuso a la internet. Desde este punto, los atacantes hicieron capturas de pantalla y accedieron a fuentes de video en vivo y archivado. Tenemos confianza moderada que los atacantes solo tuvieron acceso a las fuentes de las cámaras que Verkada administra con sus servicios en la nube. Esto se basa en algunos de los clientes de Verkada que confirman que ninguno de sus sistemas de almacenamiento de video se puso en riesgo con los ataques y que solo se expusieron las cámaras conectadas a sus servicios en la nube. Otros clientes de Verkada que se vieron impactados fueron la cárcel de Madison County, en Huntsville, Alabama; el centro de detención de Graham County de Arizona y una estación de policía sin identificar en Stoughton, Massachusetts. Los TTP que se identificaron en el ataque, incluyeron: cuentas válidas, capturas de video y de audio.

Es posible que el ataque a los sistemas de vigilancia por video haya sido parte de una operación de acceso más compleja. El 17 de enero de 2017, dos individuos rumanos poco sofisticados vulneraron las cámaras del Departamento de Policía Metropolitano de Washington, D.C. en un plan de ransomware sin éxito.14 Esto dio como resultado una pérdida de disponibilidad de cuatro días para las cámaras, ya que se desconectaron como un esfuerzo de remediación. Los actores tomaron como objetivo las cámaras de vigilancia con la intención de utilizarlas como un punto de apoyo hacia las redes adyacentes y utilizaron el RDP para moverse lateralmente desde las cámaras puestas en riesgo hacia las 123 computadoras conectadas.

Los atacantes cometieron varios errores, incluyendo elegir enviar ransomware a través de 179,000 correos electrónicos individuales utilizando un servicio de mensajería electrónica por lotes que puso en riesgo al controlador del dominio y ejecutó el ransomware desde dicha posición elevada.15 Los actores también mostraron pobre seguridad operacional al utilizar una cuenta de Gmail con el nombre de uno de ellos como dirección de recuperación para una cuenta separada que estaba ligada al ataque, demostrando su falta de sofisticación. No se reportó el método inicial de acceso para el ataque en Washington D.C. Si bien este intento no tuvo éxito, ejemplifica cómo las redes de cámaras IP podrían ser únicamente el objetivo inicial de los atacantes en ocasiones poco usuales.

DEFENSAS ACTUALES Y RECOMENDADAS

Los atacantes que más probablemente toman las soluciones de video fijo como objetivo suelen tener poca sofisticación. Por lo tanto, asegurarse de requerir controles de seguridad básicos a nivel del producto, así como garantizar que proveedores de terceros utilicen las mejores prácticas al trabajar con sus clientes, puede ayudar a inhibir y repeler la mayoría de los ataques.

Las cámaras de vigilancia fijas bien aseguradas deberían enviarse sin contraseñas predeterminadas. También deberían tener firmware cifrado y firmado. Idealmente, cada familia de cámaras debería tener una llave de cifrado derivada y única que pueda revocarse a voluntad. Adicionalmente, las cámaras deberían enviarse con tarjetas de cifrado integradas para mitigar el impacto de robo e intervención. Los usuarios finales, sin embargo, deben garantizar que parchan y actualizan sus cámaras desde una fuente proporcionada por el proveedor para asegurarse de que no se expongan a ninguna vulnerabilidad o proeza conocidas, las cuales burlen los controles de seguridad.

Al final, la consistencia y profundidad de la seguridad recae en los usuarios finales. Por ejemplo, incluso cuando se asegura un producto, si no hay una longitud de contraseña o requisito de complejidad de la misma para acceder a este, la barrera de acceso se reduce significativamente debido al riesgo de las credenciales filtradas o expuestas. La falta de conocimiento que circunda la conectividad de las cámaras IP a la internet dio como resultado el que hubiera una cantidad significativa de usuarios que no parcharon sus cámaras, así como habitualmente no las clasifican como parte de sus sistemas de OT. Si bien muchas de las cámaras son inherentemente seguras, estas requieren una administración e instalación efectivas adicionalmente a las soluciones de monitoreo integral y constante.

Con base en los eventos como el ataque a Verkada, es crítico que los sistemas de cámaras IP, ambientes en la nube y de desarrollo se aíslen de la internet abierta. No hay ninguna razón legítima conocida para que una cámara IP permita tráfico de HTTP o Telnet para los sistemas desprotegidos, sin monitorear y no autorizados. Se debe validar a los proveedores de terceros para comprobar que siguen mejores prácticas. Esto ayudará a asegurar que aquellos que ayudan a instalar y configurar los productos de cámaras de vigilancia a los clientes sean capaces y tengan la voluntad de utilizar las mejores prácticas de seguridad para proteger la misión de sus clientes.

El historial de ataques a los servicios de video ha resaltado la importancia del control de accesos. Se debe limitar el acceso de los proveedores para que solo ocurra cuando el cliente lo permita y solo durante sesiones individuales. Aún más, se recomienda que se realicen auditorías y pruebas de penetración con frecuencia y que el acceso otorgado se monitoree cuidadosamente para garantizar que esto siga siendo así.

Adicionalmente a separar las redes de cámaras IP y ambientes en la nube de los sistemas abiertos a la internet, también se deberían aislar de las redes empresariales adyacentes, incluyendo los ambientes de DevOps. En el momento del despliegue, se considera como mejor práctica el limitar el acceso hacia y desde las redes de video, lo cual se debe compartir mediante la documentación del producto con los potenciales vendedores de terceros. Esto puede ayudar a mitigar los riesgos potenciales a gran escala en caso de que las redes de cámaras IP se utilicen para obtener oportunidades de acceso a las redes de consumidores u organizacionales más grandes.

LECTORES DE PLACAS VEHICULARES (LPR)

DIRECCIONAMIENTO PREVIO E INTRUSIÓN EN DATOS Y SISTEMAS LPR

Identificamos cuatro incidentes que impactan el espacio de los Lectores de Placas Vehiculares (LPR, por sus siglas en inglés) desde 2015, adicionalmente a la identificación de sistemas LPR vulnerables y expuestos mediante escaneos de Shodan. La mayoría de estos casos involucró a los dispositivos, bases de datos o portales web que estaban abiertos a la internet, sin requerir autenticación. Uno de los cuatro incidentes ocurrió en abril del 2020.16 Nuestro equipo solo descubrió un caso de un atacante que puso en riesgo un negocio de LPR: un ataque de ransomware contra Perceptics en mayo del 2019. El grupo de extorsión Team Snatch puso en riesgo a Perceptics en lo que fue uno de los primeros ejemplos de grupos de extorsión que utilizan tanto ransomware como robo de datos como una táctica y que filtró 449 gigabytes de datos de esta empresa.

Esto incluyó a los archivos que pertenecían a uno de los clientes de Perceptics, la Agencia de Protección de Fronteras y Aduanas. Los datos que robaron incluían fotos de rostros y licencias de más de 100,000 viajeros que entraron y salieron de Estados Unidos. No sabemos qué métodos utilizó el atacante para acceder a la red de Perseptics. No hay indicaciones de que esta brecha se debiera a una vulnerabilidad en el mismo conjunto de tecnologías de LPR o de que la motivación del atacante fuera la participación de la empresa en el negocio de LPR. Cuando Perceptics no pudo pagar la cantidad solicitada, el Team Snatch proporcionó los archivos a los moderadores del sitio hactivista de información filtrada, DDoSecrets. Los moderadores de DDoSecrets publicaron entonces los datos de Perceptics en junio del 2019. Este ataque ocasionó que CBP prohibiera que la organización y los contratistas federales siguieran utilizando a Perceptics.[17]

CIBERCRIMINALES

Vender información de identificación personal financiera desde redes en riesgo, computadoras individuales infectadas, bases de datos filtradas o ataques de phishing sigue estando entre las principales prioridades de los cibercriminales.

En el año anterior, nuestro equipo encontró muy pocas conversaciones dentro del ámbito criminal clandestino con respecto a la tecnología, compañías u otros productos de LPR. Nuestra investigación en la dark web y el código abierto no identificó ningún foro criminal dedicado ni grupo que se enfocara en las intrusiones de LPR ni al mal uso de los datos de placas derivado de los datos registrados de LPR. No encontramos conversaciones en foros de la dark web sobre la planificación de ataques directos a empresas cuyas operaciones de negocio principales se enfocan en la creación o mantenimiento de tecnologías de LPR.

En vez de esto, identificamos una tendencia de los atacantes clandestinos para estar dispuestos a compartir enlaces hacia los recursos o reportes de código abierto para ayudarles a identificar dispositivos LPR vulnerables o dispositivos del IoT, particularmente, en los repositorios de código tales como GitHub.[18]

Sí se encontraron dentro de mercados clandestinos prominentes tales como Genesis Store, Russian Market o Amigos Market múltiples referencias a compañías que venden productos LPR, pero estas probablemente estaban vinculadas a intrusión en cuentas de clientes más que en cuentas administrativas. Más aún, los participantes interesados en componentes más técnicos dentro de la tecnología del IoT, específicamente, los sistemas de cámaras de CCTV, están utilizando foros clandestinos y servicios de mensajería más ampliamente en vez de productos o datos de LPR, lo cual indica que para los cibercriminales hay una falta de valor financiero y datos en las tecnologías de LPR.

No identificamos referencias específicas al uso indebido de tecnología LPR en manos de criminales. En vez de esto, un atacante podría utilizar la información que se está compartiendo y discutiendo podría usarse por actores maliciosos para obtener conocimiento sobre los componentes técnicos, así como conocer mejores prácticas de otros participantes.

> Las discusiones sobre ataques directos planificados a empresas cuyas operaciones comerciales principales giran en torno a la creación o el mantenimiento de la tecnología LPR no se descubrieron en los foros de la web oscura.

HACKTIVISTAS

La LPR sigue siendo una tecnología controversial, ya que los críticos afirman que representa una intrusión y vigilancia cada vez mayor que violenta el derecho a la privacidad.[19] Creemos que esto podría motivar a los atacantes hacktivistas a fijar los sistemas LPR como objetivo con la intención de generar publicidad y exponer sistemas inseguros. Es probable que los proveedores y usuarios de LPR representen un objetivo para los atacantes hacktivistas con motivaciones políticas por razones similares al ataque a Verkada: dar un golpe contra el exceso de confianza en la vigilancia de espacios públicos. Dicho esto, no obtuvimos información específica sobre la intención de atacar sistemas LPR.

Examinamos los foros de código abierto, servicios de mensajería y sitios web relacionados con la seguridad en búsqueda de contenido relacionado con la tecnología LPR, así como los productos de proveedores de LPR. En nuestra investigación, identificamos diversos foros de marcas específicas, en donde los usuarios debatieron los temas antes mencionados, pero no identificamos contenido considerado como malicioso o relacionado con la vulneración de LPR o que buscara dañar los sistemas antes mencionados. El análisis de una muestra de hilos en foros ubicó los siguientes temas:

- No identificaron a usuarios que debatieran las vulnerabilidades de los componentes LPR, específicamente en el software que podría utilizarse para propósitos maliciosos.
- Conversaciones sobre los LPR, tanto en lo relativo a los elementos básicos de la tecnología como la forma en que supuestamente exacerba el problema de exceso de vigilancia.

Nuestro equipo observó una disminución general de la actividad internacional de los hacktivistas, en tanto el panorama de hacktivismo se replegó de una participación pública más amplia, regresando a sus orígenes como una práctica de grupos más pequeños compuestos por individuos comprometidos. Como tal, los ataques relacionados con el hacktivismo a menudo dan como resultado uno de los siguientes efectos:

- Negación de servicio
- Desfiguración de los sitios web y portales de contacto al público
- Diseminación pública de datos sensibles

ESTADOS NACIONALES

No descubrimos ningún caso especial de atacantes patrocinados a nivel del Estado que buscaran acceder a sistemas o datos LPR de forma encubierta. Creemos que por lo menos algunos grupos patrocinados por estados están interesados en obtener dichos datos para propósitos de obtener información, por ejemplo, que les permita rastrear movimientos de las personas de interés en otros países. Sin embargo, en general creemos que obtener este tipo de datos no se considera prioritario.

VULNERABILIDADES COMUNES Y MÉTODOS DE INFECCIÓN

Las cámaras lectoras de placas vehiculares can bajo la sobra de los dispositivos del IoT. A menudo, se ataca y pone en riesgo a estos dispositivos para crear una botnet, frecuentemente a través del uso excesivo de credenciales predeterminadas o mediante atacantes que descifran las contraseñas por fuerza bruta. Estas botnets a menudo se utilizan para llevar a cabo ataques de DDoS. Sin embargo, la mayoría de los riesgos observados para los mismos sistemas de LPR simplemente fueron el resultado de redes de proveedores de servicios expuestas, las cuales no contaban con seguridad de autenticación.

Un tema que nuestro equipo identificó dentro del mundo clandestino fue el interés de los atacantes por compartir técnicas de investigación para identificar las tecnologías del IoT susceptibles de ser vulneradas. Sin embargo, las menciones de la tecnología LPR en el contexto de estas búsquedas siguieron siendo mínimas.

Descubrimos una instancia de estas vulnerabilidades que pertenece específicamente a las cámaras de LPR. El 21 de enero de 2021, un investigador de la firma macedonia Zero Science Lab publicó los detalles de nueve vulnerabilidades que afectaron a varios modelos de cámaras LPR que vende Selea, un diseñador y fabricante italiano. Parece que Selea es una compañía relativamente pequeña sin un gran valor en el mercado. Las vulnerabilidades se publicaron posteriormente en varios sitios de repositorios de vulnerabilidades y proezas, tales como exploit-lab.

Las nueve vulnerabilidades incluyeron una vulnerabilidad de navegación por directorios sin autenticación, la cual permitiría que los atacantes recuperaran credenciales, así como una vulnerabilidad de inyección de comandos remotos para autenticación posterior.

Estas dos vulnerabilidades podrían haberse encadenado fácilmente entre ellas para permitir una ejecución de código remoto sin autenticar. Sólo se encontró una mención de estas vulnerabilidades en la dark web o en los foros clandestinos y no hay más contexto sobre esta referencia para indicar si tuvo algún interés significativo. No descubrimos ninguna indicación de que estas vulnerabilidades se hayan aprovechado o se esté haciendo activamente en la actualidad.

PANORAMA FUTURO DE LA INDUSTRIA DE LOS LPR

Es posible que veamos otros casos en el futuro de datos LPR con una protección inadecuada, incluyendo dispositivos o portales de entrada que tengan un acceso abierto a la internet.
Así como en el caso de Perceptics, las compañías de LPR pueden convertirse en objetivos de campañas de ransomeware, aunque no creemos que su participación específica en la tecnología LPR es lo que facilitaría o motivaría dichos ataques. Debido a la naturaleza controversial de aspectos de dicha tecnología, la LPR seguirá representando un objetivo potencial para atacantes hacktivistas. Aunque se encontró poca información en la dark web y en los foros de clearnet con respecto a plneación de ciberataques y el aprovechamiento de vulnerabilidades en la tecnología LPR, creemos que es altamente probable que los foros sigan atrayendo a atacantes interesados en las tecnologías del IoT y en los avances tecnológicos de la industria.

ARMADO CON CONOCIMIENTO

CÓMO ENFRENTAR CON CONFIANZA LOS RETOS CIBERNÉTICOS DE LA ACTUALIDAD

Conforme llegamos al segundo año de la pandemia del COVID-19, los datos y los sistemas de seguridad pública se están integrando cada vez más, creando retos nuevos para los equipos de seguridad mientras se defienden contra criminales, estados nacionales, hacktivistas y otros.

Estos ciberdelincuentes saben que los servicios de emergencia seguros y confiables son esenciales para combatir la pandemia y mantener a los ciudadanos a salvo de otros de peligros cotidianos. Eso es lo que los hace objetivos tan atractivos.

Esperamos que la información contenida en este reporte fortalezca a las organizaciones de seguridad pública para repeler a los adversarios con conocimiento práctico sobre los métodos, intenciones y operaciones que utilizan.

Hoy en día, este conocimiento es un fundamento clave de todos los productos y servicios que desarrolla Motorola Solutions. Nuestros clientes enfrentan cada vez más ataques cibernéticos peligrosos y sofisticados.

Pero no tienen que enfrentar esta amenaza solos. Al estar equipados con el conocimiento que contiene este reporte de Ciberamenazas a la Seguridad Pública del 2021 de Motorola Solutions, están listos para enfrentar con confianza los retos cibernéticos de la actualidad

GLOSARIO DE TÉRMINOS

TÁCTICAS, TÉCNICAS Y PROCEDIMIENTOS QUE NO SE ENCUENTRAN EN EL MARCO DE TRABAJO DE ATT&CK DE MITRE

- **Líneas administrativas:** números telefónicos de entrada específicos que pertenecen a los PSAP (tales como los números 1-800). Estas líneas existen adicionalmente a las líneas de emergencia que se utilizan para enrutar las llamadas al 9-1-1.
- **9-1-1 directo:** los atacantes podrían llamar a las líneas de emergencia directamente (tal como al 9-1-1 en los Estados Unidos) para apuntar a los PSAP locales con sus ataques de Negación de Servicio Telefónico.
- **Extorsión / publicación de datos:** los atacantes podrían robar datos para extorsionar a las víctimas por su divulgación. En estos casos, los atacantes podrían publicar parte de los datos en sitios personalizados diseñados para compartirlos. Se observa que este comportamiento a menudo se asocia con grupos de extorsión.
- **Robo de llaves y hardware:** un método común de los atacantes para obtener acceso a transmisiones de LMR. Los atacantes podrían utilizar radios o llaves de cifrado de hardware robadas para vigilar las comunicaciones cifradas entre el personal de primera respuesta y los oficiales federales. Los atacantes también podrían utilizar las radios o llaves de cifrado de hardware robadas para llevar a cabo ataques de Negación de Servicio en Transmisiones.
- **Acceso inherente:** individuos involuntarios o con intención maliciosa al interior de la organización son un elemento usual que pone en riesgo las transmisiones o los sistemas de LMR. Acceso inherente es el término que se utiliza para describir los ataques o eventos en donde no se requirió una acción externa para obtener acceso a los LMR.
- **Negación del servicio de transmisión:** los atacantes podrían interrumpir las comunicaciones de LMR por razones políticas, ideológicas o financieras al transmitir sonidos e información falsos, confusos o arbitrarios a través de los canales de voz cifrados y descifrados. Esta táctica se utiliza a menudo en conjunto con el robo de llaves o hardware, especialmente en las instancias en donde se interrumpió el canal de comunicación cifrado.
- **Negación del servicio telefónico:** un ataque de Negación del Servicio Telefónico (TDoS) es un intento por lograr que un sistema telefónico quede indispuesto para los usuarios previstos, previniendo la entrada y salida de llamadas. Esto se logra cuando los atacantes consumen todos los recursos telefónicos con éxito para que no quede ninguna línea telefónica sin ocupar.

NIVELES DE CONFIANZA ANALÍTICA

- **Confianza alta:** generalmente indica juicios que se basan en información de alta calidad o en donde la naturaleza del problema hace posible dar un juicio sólido. Sin embargo, un juicio de "confianza alta" no constituye un hecho infalible o una certeza y aun así conlleva el riesgo de ser erróneo.
- **Confianza moderada:** generalmente significa información factible y de fuentes fidedignas, pero que no tiene una calidad o confirmación suficientes para garantizar un nivel de confianza alto.
- **Confianza baja:** generalmente significa que se utilizó información cuestionable o poco plausible, que está demasiado fragmentada o tiene una confirmación insuficiente para realizar inferencias de análisis sólidas o que existen dudas o problemas relevantes con respecto a las fuentes.

FUENTES

1 https://unit42.paloaltonetworks.com/ransomware-threat-report-highlights/

2 https://www.cbc.ca/news/canada/toronto/toronto-police-tow-truck-radios-1.5622069

3 https://pages.nist.gov/mobile-threat-catalogue/background/mtc-overview/

4 https://www.ic3.gov/Media/Y2021/PSA210217

5 https://www.coveware.com/phobos-ransomware-payment

6 https://www.cyberscoop.com/911-call-center-ddos-dhs-maricopa-county/

7 Kalbo, Naor et al. "The Seguridad of IP-Based Vigilancia Por Video Systems." Sensors (Basel, Suiza) vol. 20,17 4806. 26 de agosto. 2020, doi:10.3390/s20174806

8 https://www.bleepingcomputer.com/news/security/hackers-access-surveillance-cameras-at-tesla-cloudflare-banks-more/

9 Alguien que no tiene el conocimiento de programación o de redes y que utiliza software existente para lanzar un ataque. A menudo, un "script kiddie" utilizará estos programas sin siquiera saber cómo funcionan o lo que pueden hacer.

10 https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html

11 https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/#:~:text=At%20its%20peak%2C%20Mirai%20infected,devices%2C%20according%20to%20our%20measurements.

12 https://www.cyber.nj.gov/threat-center/threat-profiles/botnet-variants/linux-irctelnet

13 Visite attack.mitre.org para obtener más detalles.

14 https://www.justice.gov/usao-dc/pr/two-romanian-suspects-charged-hacking-metropolitan-police-department-surveillance-cameras

15 https://www.justice.gov/usao-dc/press-release/file/1021186/download

16 https://www.theregister.com/2020/04/28/anpr_sheffield_council/

17 https://www.cyberscoop.com/perceptics-cbp-suspends-contractor/

18 Un sistema de dispositivos de cómputo, máquinas mecánicas y máquinas digitales, objetos, animales o personas interrelacionados que proporcionan identificadores únicos y la capacidad de transferir datos por una red sin requerir una interacción de humano a humano o humano a computadora.

19 https://www.bloomberg.com/news/articles/2018-12-06/why-privacy-advocates-fear-license-plate-readers

Para obtener más información sobre nuestros servicios de ciberseguridad, contacte a su representante de ventas de Motorola Solutions o visite: **motorolasolutions.com/cybersecurity**

MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, Il 60661 U.S.A. **motorolasolutions.com**

MOTOROLA, MOTO, MOTOROLA SOLUTIONS y el logotipo de la M estilizada son marcas comerciales o marcas comerciales registradas de Motorola Trademark Holdings, LLC y son utilizadas bajo licencia. Todas las demás marcas comerciales pertenecen a sus respectivos propietarios. © 2021 Motorola Solutions, Inc. Todos los derechos reservados. 11-2021 [CK05]