AMEAÇAS CIBERNÉTICAS PARA A SEGURANÇA PÚBLICA 2021

FOCO DO PRODUTO

Percepções da Equipe de Inteligência em Ameaças da Motorola Solutions

MOTOROLA SOLUTIONS


D.A.ACOSTA
AGENTE
PFA

Como líder mundial em tecnologia de segurança pública, a Motorola Solutions constrói soluções altamente inovadoras para aplicação da lei, combate a incêndios, EMS, 9-1-1, e outros órgãos estaduais e federais. Nosso compromisso em fornecer os melhores produtos e serviços para o setor público, com foco na segurança cibernética, nos dá uma visão direta sobre as ameaças cibernéticas que desafiam de forma única os primeiros socorristas em todo o mundo. Desde 2018, a Equipe de Inteligência em Ameaças da Motorola Solutions tem compilado anualmente suas pesquisas e análises para compartilhar diretamente esta visão com organizações de segurança pública

Em 2021, ao entrarmos no segundo ano da pandemia da COVID-19, a segurança pública, como outros setores, tornou-se mais interligada, com sistemas e dados anteriormente díspares e cada vez mais integrados. No relatório anual deste ano, compartilhamos nossas descobertas sobre como essa interconexão cria novos riscos, exacerba as questões conhecidas e requer novos níveis de vigilância.

Para compilar este relatório, a Equipe de Inteligência em Ameaças utilizou dados proprietários, anonimizados juntamente com a inteligência cibernética de fonte aberta e fechada de 1º janeiro a 15 de setembro de 2021, além de uma pesquisa abrangente sobre o espaço tecnológico de segurança pública para identificar as ameaças mais urgentes e significativas, os atores da ameaça e os riscos para os serviços de emergência.

Conhecimento é poder. Nosso objetivo é capacitar líderes e profissionais com as informações necessárias para minimizar riscos e estar um passo à frente dos desafios cibernéticos mais significativos em todo o ecossistema de missão crítica de segurança pública. Ao compartilhar nossas pesquisas, acreditamos que este relatório poderá melhorar a segurança e a conscientização das agências e organizações críticas encarregadas de nos manter a todos em segurança.

ÍNDICE

SUMÁRIO EXECUTIVO

Identificar os atores da ameaça e seu artesanato associado nos ajuda a fazer recomendações mais específicas para a segurança.

Com o segundo ano da pandemia COVID-19 no mundo, nos tornamos mais ágeis, adaptáveis e interligados. Nossas ferramentas também o fizeram. Essas ferramentas nos permitiram ser produtivos e eficientes, não importando onde estivéssemos. Para a segurança pública, isto significava uma resposta de emergência confiável e eficiente, ao mesmo tempo em que evitávamos ameaças crescentes à disponibilidade, integridade e confidencialidade. Tudo, desde rádios, plataformas de comunicação, conjuntos de comunicação e sistemas de vigilância por vídeo, tornou-se mais fundamentalmente vinculado, proporcionando maior inteligência e recursos simplificados. Entretanto, os benefícios destas ferramentas de próxima geração não vêm sem risco.

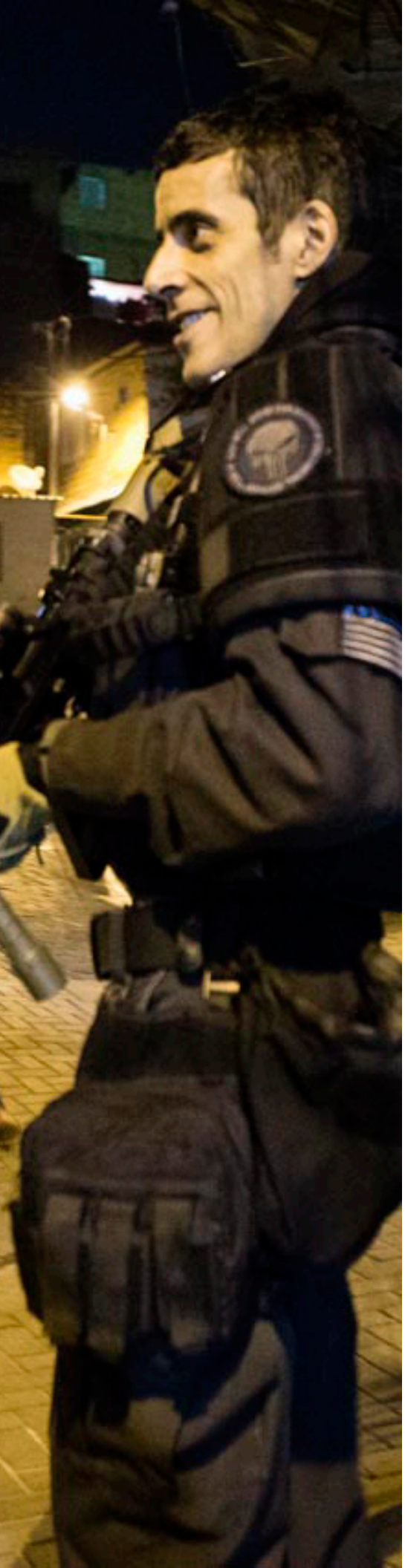
Em 2021, as ameaças cibernéticas de segurança se tornaram mais sofisticadas, persistentes e difundidas. Os pagamentos de resgate aumentaram 82% globalmente, enquanto as consequências dos ataques de extorsão aumentaram devido à técnica adicional de roubo de dados.1 Nossa equipe de Inteligência em Ameaças concentrou-se em compreender melhor as ameaças que frequentemente visam a segurança pública. Identificar os atores da ameaça e suas artes associadas nos ajuda a fazer recomendações mais específicas para a segurança.

Os Pontos de Atendimento de Segurança Pública (PSAPs), críticos para o encaminhamento de chamadas de emergência, continuaram sendo o alvo de segurança pública mais frequente, mais comumente atingido com ataques de Telephony Denial-of-Service (TDoS) de baixo impacto. Como resultado da interconectividade cada vez maior com outros sistemas e dispositivos, o rádio móvel terrestre (LMR) viu um ligeiro aumento no número de compromissos e incidentes de segurança, incluindo infecções por malware e ataques de resgates. Ferramentas de vigilância por vídeo, tais como leitores de placas e câmeras de segurança fixas, representam um alvo provável para atores relativamente pouco sofisticados que podem tentar aumentar o tamanho das redes de bots existentes ou fazer uma declaração política através de violações de dados.

O KIT DE FERRAMENTAS DE SEGURANÇA PÚBLICA

RÁDIO MÓVEL TERRESTRE

O rádio móvel terrestre (LMR) permite a comunicação bidirecional 'push-to-talk' entre transceptores de rádio e pode ser construído em muitas variações diferentes, incluindo base fixa, montada em veículo e de mão. Ele é utilizado em uma variedade de indústrias, incluindo comunicações de missão crítica de segurança pública e comunicações privadas para indústrias comerciais, tais como petróleo e gás. Uma vez que a LMR permite uma comunicação segura e instantânea, ela é freqUentemente um método primário de comunicação nestas indústrias, particularmente em ambientes onde o serviço celular não é prático porque é limitado ou inexistente.



APCO INTERNATIONAL SISTEMAS PROJECT 25 (P25)

Os sistemas tradicionais ou enclaves P25 LMR não estão totalmente isolados da Internet e não devem ser considerados como intrinsecamente seguros. Embora eles existam mais comumente atrás de dois firewalls, temos uma confiança moderada de que a topografia de rede dos sistemas de enclaves e os relatos altamente privilegiados poderiam permitir o acesso de um paciente ou invasor persistente em raras ocasiões. Esta avaliação é baseada nos esquemas de rede disponíveis e nas configurações de implantação conhecidas.

A má configuração e o não aproveitamento total das características de segurança disponíveis são as armadilhas mais comuns nos sistemas LMR P25. O uso de contas de administrador incorporadas em vez de contas não privilegiadas para uso normal, e políticas de firewall ausentes ou mal configuradas para segmentar a rede LMR de redes adjacentes são as configurações errôneas mais relatadas com maior frequência para os sistemas P25. Entretanto, em alguns casos, os sistemas P25 que foram configurados corretamente não estavam aproveitando todos os recursos de segurança disponíveis nativos de seus sistemas, tais como sistemas de prevenção de intrusão (IPS) em hosts, o que permitiu que os invasores passassem despercebidos. Incentivamos todos os usuários do P25 a trabalhar com seus fornecedores para garantir que eles entendam e apliquem o maior número possível de capacidades de segurança que estão disponíveis nativamente.

A exploração de vulnerabilidades em soluções de acesso remoto pode permitir o acesso ou controle sobre um ambiente central P25. Desde o início da pandemia de Covid-19, a comunidade global de cibersegurança tem visto um esforço concentrado de atores maliciosos para encontrar e explorar vulnerabilidades em soluções de acesso remoto, tais como VPNs.
Embora não seja única aos sistemas P25, as soluções VPN de Palo Alto, Fortinet e Pulse Secure servem como exemplos que foram relatados pela CISA em 2020 e 2021, como tendo vulnerabilidades que foram exploradas por atores maliciosos. As VPNs não são intrinsecamente inseguras. Entretanto, quando as vulnerabilidades são conhecidas, a aplicação de mitigações recomendadas deve ser priorizada e, em todos os casos viáveis, a autenticação multi-fator deve ser usada para suas contas.

SISTEMAS TETRA

Quando comparada à P25, o TETRA tem preocupações de segurança separadas. Com base em observações, os ambientes TETRA permitem conexões remotas em raras ocasiões.

Existe um potencial de administradores TETRA que executam conexões de fora de suas redes de TI, através de firewalls, em sistemas TETRA. Essas conexões são em geral gerenciadas por soluções de acesso remoto de terceiros.

Tanto nos casos de ambiente TETRA como de APCO P25, as vulnerabilidades nesse firewall ou nas soluções de acesso remoto poderiam permitir que um invasor abusasse dessas conexões remotas.

Os usuários devem confiar consistentemente nas melhores práticas, tais como a aplicação regular de patches, auditoria regular e rotação de credenciais de acesso, e desativação de portas e serviços não utilizados para ajudar a mitigar este problema.

DESENVOLVIMENTO DE ATAQUE CIBERNÉTICO EM RÁDIO MÓVEL TERRESTRE

Realizamos a última revisão abrangente do cenário de ameaças LMR em meados de 2020. Desde então, a mudança mais significativa nos ataques aos sistemas LMR é um aumento mínimo em Broadcast-Denial-of-Service (BDoS) e um aumento mínimo em Data Encrypted for Impact to LMR systems. Os ataques BDoS ocorreram em conjunto com uma agitação social mais ampla, especificamente quando os governos locais decretaram o toque de recolher e os protestos liderados pelos cidadãos estavam em andamento, especialmente durante o verão de 2020. É altamente provável que estes ataques BDoS tenham sido conduzidos em resposta direta a protestos generalizados e tenham sido motivados ideologicamente. Os ataques de resgate com impacto na LMR foram quase certamente motivados por razões financeiras e pareciam ser viabilizados por configurações errôneas e senhas padrão. Tanto os ataques BDoS e de resgate observados colocaram a negação de disponibilidade (DoA) como o impacto de ataque mais comum, com quatro em cada cinco incidentes resultando em DoA. Portanto, é avaliado com confiança moderada que qualquer ataque bem sucedido financeiro ou ideologicamente motivado à LMR é mais provável que resulte em um impacto na disponibilidade dos sistemas LMR, seja através da interrupção das comunicações por via aérea ou pela criptografia de servidores de gerenciamento de rádio.

Observamos anteriormente criminosos não tecnicamente sofisticados usando Hardware ou Roubo de Chaves como forma de obter acesso às comunicações criptografadas das autoridades policiais e de criar seus próprios canais privados. Essa tendência tem continuado desde meados de 2020. Em 22 de junho de 2020, o Departamento de Polícia de Toronto anunciou que seus investigadores haviam descoberto um esquema para fornecer rádios policiais roubados aos motoristas de reboque da cidade, e 11 indivíduos foram acusados. A operação criminosa colocou equipamentos policiais criptografados nas mãos de vários motoristas que trabalhavam para várias organizações de reboque de Toronto.

Esses motoristas planejaram usar os rádios para pesquisar as comunicações policiais, ganhando assim uma vantagem em encontrar e chegar aos locais de acidentes veiculares antes dos concorrentes. Este "sistema de alerta precoce" foi especialmente valioso para rebocar motoristas de caminhão durante o auge da pandemia da COVID-19 em Toronto, pois havia menos motoristas na estrada, o que reduziu o número de acidentes em geral. Os investigadores apreenderam três rádios, seis caminhões de reboque e uma arma como parte das prisões. A Polícia de Toronto prendeu pelo menos um oficial em conexão com os furtos por rádio.2 Com base na prevalência da tática de Hardware ou Roubo de Chave em compromissos não sofisticados, avaliamos com alta confiança que este método permanecerá popular, especialmente entre indivíduos ou grupos que buscam fugir ou monitorar a aplicação da lei.

Durante a resposta a incidentes e investigações de ataques aos sistemas LMR, a Equipe de Inteligência em Ameaças da Motorola Solutions conseguiu identificar a espionagem mais comumente utilizada pelos invasores, o que incluiu a varredura de blocos IP para o sistema alvo, bem como a varredura de vulnerabilidade como parte de seus esforços iniciais de reconhecimento. Em casos como o exemplo de Toronto acima, os agentes responsáveis pelo incidente de cibersegurança menos sofisticados frequentemente dependiam do "acesso inerente", usando informantes internos para fornecer rádios roubados ou chaves de criptografia. Enquanto isso, os agentes responsáveis pelo incidente de cibersegurança mais sofisticados usaram métodos tradicionais de acesso, tais como o comprometimento de serviços remotos externos e exploração de aplicativos voltados para o público para invadir redes LMR vulneráveis e expostas e sistemas adjacentes. Uma vez nas redes alvo, os invasores foram observados obtendo contas de domínio padrão para privilégios elevados.

Os invasores foram identificados removendo os indicadores de hosts durante um ataque para evitar a detecção e a atribuição. Em todos os casos observados, pesquisados ou avaliados de comprometimento da LMR, os invasores conduziram um ataque BDoS ou executaram um resgate para criptografar os dados quando não procuravam vigiar as comunicações da polícia ou estabelecer seu próprio canal clandestino.

Vulnerabilidades nesse firewall ou nas soluções de acesso remoto poderiam permitir que um invasor abusasse dessas conexões remotas. Recomenda- se que os usuários confiem consistentemente nas melhores práticas, como a aplicação de patches regulares e a desativação de portas e serviços não utilizados, para ajudar a mitigar este problema.

MAPEAMENTO DE LMR MITRE ATT&CK

RECONHECIMENTO	ACCESO INICIAL	EXECUÇÃO	PERSISTÊNCIA	ESCALONAMENTO DE PRIVILÉGIO	EVAÇÃO DA DEFESA
Varrduta de Blocos de IP	Hardware/Roubo de Chaves	PowerShell	Serviços Remotos Externos	Controle de Desvito de Conta do Usuário	Remoção de Indicatorsobre Host
Varredura de Vulnerabilidade	Acesso Inerentes (Ameaça de Insider)	Windows Command Shell	Criar of Modificar o Windows Process	Injeções do Processo	Desativar ou Modificar Ferramentas
	Replicação Por mídia Removíceil	Unix Shell		Exploração para Escalonamento de Privilégio	Desativar Registro de Windows Event
	Serviços Remotos Externos	Instrumentação de Gestão do Windows (WMI)			Arquivos ou Informações Ocultas
	Aplicatico de Exploração Public-Facing	Execução de Serviços			Corresponder Nome ou Local Legítimo
	Contas Padrão	API Nativo			Modificar Regsitro
	Contas de Domínios	Python			Msiexec Execution Assinado
	Dependências de Software de Comprometimento e Ferramentas de Desenvolvimento				Regsvr32 Execution Assinado
	Cadeia de Fornecimento de Software de Comprometimento				Rundll32 Execution Assinado

CREDENIAL DE ACESSO	DESCOBERTA	MOVIMENTO LATERAL	COLETA	COMANDO & CONTROLE	EXFILTRAÇÃO	IMPACTO
Pulverização de Senha	Descoberta de Processo	Transferência Lateral de Ferramentas	Captura de Áudio	Canal Criptografado	Exfiltração Sobre o Canal C2	Broadcast-denial-of-service (BDoS)
Stuffing de Credenciais	Varredura de Seriço de Rede	Replicação por Mídia Removível	Dados do Sistema Local	Proxy Externo	Exfiltração sobre o Protocolo Sym- Métrica Encriptada Não-C2	Dados Criptografados para Impacto
Adivinhação de Senha	Descoberta de informações do sistema	Serviços Remotos (quando aplicável)	Dados do Repositório de Configuração	Porta Não Padrão	Exfiltração sobre o Protocolo Asym- Métrica Encriptado Não-C2	Encerramento/ Reboot do Sistema
Dumping do Credenciamento de Sistemas Operacionais	Sistema de Descoberta de Serviços				Exfiltração sobre Protocolo Não-Criptografado/Não-Criptografado de C2	Destruição de Dados
Credenciais em Arquivos	Descoberta de Grupos de Domínios					Seqüestro de Recursos
	Descoberta das Conexões de Rede do Sistema					Parada de Serviço
	Compartir la red					Inibir a Recuperação do Sistema
	Descoberta de Arquivos e Diretórios					Network-denial -of- service
	Sniffing de Rede					

LEGENDA
Propenso
Provável
Possível
Improvável / Raro

AÇÕES RECOMENDADADAS

A natureza cada vez mais conectada dos sistemas LMR não se conjuga bem com o aumento de invasores sofisticados. Esta combinação requer operadores e técnicos da LMR para garantir uma abordagem de segurança em camadas, aplicada e abrangente. Também exige que os usuários LMR garantam que esses controles de segurança nativos sejam implementados no momento da instalação, durante a operação, e complementados com controles administrativos, políticas e procedimentos.

A autenticação multi-fator deve ser habilitada e aplicada para todas as contas disponíveis que acessam a DMZ e o núcleo de um sistema LMR. Dispositivos de acesso comprometidos podem introduzir uma variedade de ameaças aos ambientes de nuvem LMR, conforme definido pelo Instituto Nacional de Padrões e Tecnologia em seu catálogo de ameaças móveis.3

Finalmente, os procedimentos para comunicar a perda ou roubo de equipamentos, auditoria de inventário regular de equipamentos de rádio, bem como para desativar esses equipamentos devem ser implementados sempre que possível. Isto pode ajudar a identificar quando o Hardware ou TTP de Roubo de Chave é utilizável por pessoas de dentro e agentes de baixa sofisticação.

CONJUNTO DE PONTOS DE ATENDIMENTO DE SEGURANÇA PÚBLICA

O PONTO DE ATENDIMENTO DE SEGURANÇA PÚBLICA

Os Pontos de Atendimento de Segurança Pública (PSAPs) são centros que processam chamadas de emergência. Eles normalmente têm cinco fluxos primários de comunicação: chamadas de entrada 9-1-1, tráfego de entrada de SMS, consultas de localização de saída, tráfego de comunicação de saída e linhas administrativas bidirecionais. Esta infraestrutura crítica permite que os atendentes de emergência sejam informados e respondam a eventos significativos que afetam o público. Com a implementação de serviços de rede telefônica baseados em IP e tecnologia em evolução, os PSAPs devem estar preparados para gerenciar ativamente possíveis ameaças de segurança cibernética, incluindo ataques de Telephony Service Denial (TDos), ransomware [ataque virtual com pedido de resgate] e outros acessos não autorizados a dados e sistemas. Com o aumento do uso de plataformas baseadas em IP e o consequente aumento da superfície de ataque, o risco de ataques de cibersegurança e outras ameaças contra os PSAPs provavelmente aumentará.

TRATEMENTO DE CHAMADAS

O tratamento de chamadas é realizado através de software baseado em IP e telefonia utilizada para aceitar, fazer fila e atender chamadas de emergência. Os sistemas de tratamento de chamadas da geração atual também podem aceitar mensagens baseadas em SMS. No futuro, espera-se que estas soluções processem outras formas de tráfego de mensagens de emergência, tais como multimídia.

Uma das ameaças mais significativas aos PSAPs são os ataques TDoS através de linhas telefônicas físicas e baseadas em IP.4 Os agentes de ameaça fazem os ataques TDoS contra linhas telefônicas 9-1-1 e administrativas, o que pode resultar em interrupções na capacidade de tratamento de chamadas. Embora estes ataques muitas vezes não sejam relatados, eles continuam sendo o tipo de ataque mais comum que temos observado envolvendo PSAPs. Estes ataques são extremamente fáceis de conduzir, exigindo pouca ou nenhuma sofisticação.

Um invasor pode conduzir uma TDoS de duas maneiras: manual e automatizada. Para ataques manuais TDoS, os agentes de ameaça devem ter acesso a um número arbitrário, mas muitas vezes alto, de telefones. Estes são telefones descartáveis pré-pagos ou telefones comprometidos com malware. Em ambos os cenários, o invasor pode afetar estes dispositivos, fazendo com que eles disquem números de emergência, inundando PSAPs com chamadas geradas manualmente.
Os ataques automatizados são mais fáceis de conduzir. Eles exigem apenas acesso a um sistema de telefonia virtual capaz de fazer um grande número de chamadas geradas por computador.

Isto pode ser feito alugando acesso a botnets de baixo custo ou mesmo executando programas simples via desktops ou outras estações de trabalho.

As motivações por trás dos ataques TDoS variam de ideológicas a financeiras ou até mesmo de notoriedade. Entretanto, os relatórios disponíveis das vítimas sugerem que é provável que os invasores de baixa sofisticação procurem principalmente ganhar dinheiro em esquemas TDoS extorquindo PSAPs por um resgate. Estes invasores TDoS com motivação financeira muitas vezes não estão filiados a grupos específicos, optando por agir sozinhos.

Os sistemas de última geração de 9-1-1 (NG9-1-1) são mais resistentes aos ataques TDoS do que os sistemas legados, pois são capazes de lidar com um número muito maior de chamadas simultâneas do que os sistemas mais antigos. Entretanto, os ataques TDoS ainda são um problema para o NG9-1-1. Enquanto os sistemas NG9-1-1 conseguem suportar a enchente de chamadas recebidas por invasores TDoS, os funcionários do PSAP no recebimento dessas chamadas não têm tanta sorte.

Em sistemas mais antigos, que não o GN9-1-1, os ataques TDoS impactaram as linhas telefônicas dos prestadores de serviços devido à carga de chamadas ser maior do que a largura de banda da telefonia. No NG9-1-1, essas chamadas fraudulentas estão sendo atendidas, resultando na necessidade de atender as chamadas. Chamadas "reais" se misturam com estas chamadas falsas, enquanto os cidadãos comuns tentam contatar os serviços de emergência. Isto resulta em pessoas tendo que esperar mais tempo para que suas ligações sejam atendidas, o que muitas vezes leva a ligações e discagens abandonadas, criando efetivamente outra TDoS dentro do ataque original.

Ao conduzir ataques TDoS contra PSAPs, os agentes de ameaça podem posicionar chamadas durante os momentos em que os defensores não conseguem responder proativamente devido ao alto volume de chamadas ou ao baixo número de funcionários. Protestos em todo o estado ou desastres naturais como incêndios florestais podem resultar em um alto número de chamadas legítimas de 9-1-1.

Enquanto isso, fora das horas de expediente e alguns feriados podem significar menos pessoal da comunicação no trabalho. Qualquer uma destas situações agravará os efeitos perturbadores dos ataques TDoS.

COMUNICAÇÃO ASSISTIDA POR COMPUTADOR (CAD)

Os dispatchers, atendentes de chamadas e operadores de 9-1-1 usam os sistemas de Comunicação Assistida por Computador (CAD) para enviar o pessoal de emergência para o local onde eles são mais necessários. Os dispatchers também usam sistemas CAD para identificar a localização e o status dos primeiros socorristas, além de priorizar e registrar as chamadas de emergência recebidas.

O Ransomware é a ameaça mais comum ao CAD, impactando os sistemas CAD de duas maneiras. A primeira é através de ataques indiretos às redes municipais e policiais. Esses ambientes municipais e policiais frequentemente funcionam como redes de base para os sistemas CAD. No caso de um ataque ransomware, os defensores podem desativar os serviços de rede como precaução, como parte da resposta a incidentes, ou durante atividades posteriores de restauração de dados.

Cada um desses cenários pode resultar em interrupções dos serviços de CAD.
A segunda maneira pela qual o ransomware pode impactar os sistemas CAD é durante um compromisso direto das próprias redes CAD. O compromisso direto é mais raro, mas ocorre - especialmente quando exacerbado por configurações errôneas ou serviços não seguros. Os compromissos diretos de redes CAD muitas vezes vêm de conexões confiáveis entre o ambiente CAD e as redes municipais ou policiais adjacentes. Eles também ocorrem quando as estações de trabalho CAD são habilitadas com conectividade à Internet de saída, uma prática que não é o padrão e não é recomendada. Finalmente, serviços de entrada, tais como conexões VPN, podem ser comprometidos em raras ocasiões, levando os agentes de ameaça a acessar os sistemas CAD a partir da Internet aberta ou de outras redes.

DESENVOLVIMENTOS RECENTES

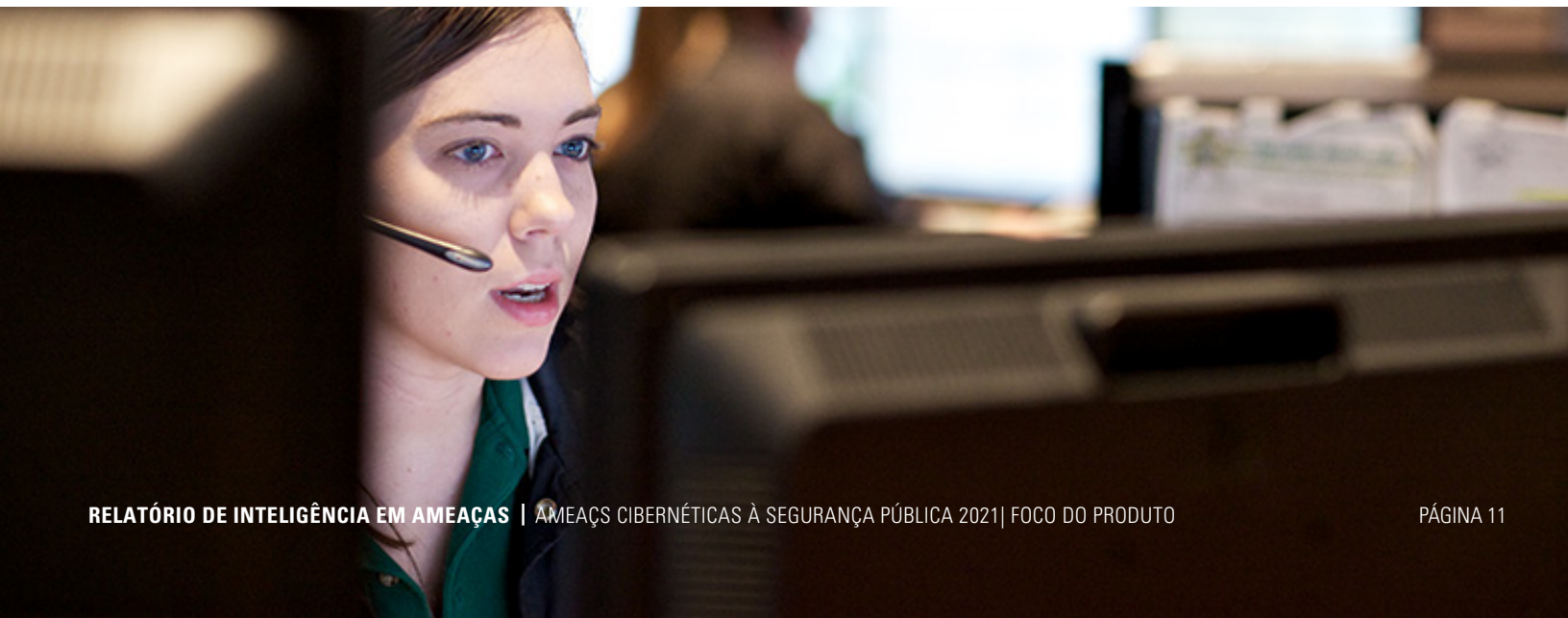
TURNOS DE ATAQUES

Realizamos a última revisão abrangente do cenário de ameaças do PSAP em agosto de 2020. Desde então, os ataques ao PSAP têm aumentado. Houve um salto de 38% nos ataques relatados no segundo semestre de 2020 e no início de 2021. Isto se deveu em grande parte a cinco ataques TDoS contra centros de comunicação nos Estados Unidos, resultando na degradação dos serviços de atendimento e tratamento de chamadas em cada instância. No período anterior, houve zero ataques TDoS reportados. Entretanto, estes eventos raramente são divulgados e, portanto, pode-se afirmar com alta confiança que os ataques TDoS provavelmente ocorreram mas não foram registrados. Uma notificação de avaliação de ameaça estatal publicada em maio de 2021 observou um "aumento generalizado de ataques de negação de serviço telefônico" para PSAPs de âmbito nacional. Com base nesta análise, o aumento observado nos ataques TDoS desde 1º de agosto de 2020, poderia indicar que há mais destes eventos ocorrendo, ou que a notificação aumentou. Não podemos determinar de forma confiável o que é verdade neste momento.

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.



ATIVIDADE DO FÓRUM CRIMINOSO

A confiança nos ataques virtuais TDoS desenvolveu-se devido à prevalência da tecnologia VoIP (Voice-over-IP), que permite aos indivíduos enviar um número arbitrário de "ligações telefônicas", sem ter que primeiro obter acesso a uma ampla gama de telefones.

A Equipe de Inteligência em Ameaças das Motorola Solutions observou indivíduos oferecendo serviços que poderiam ser utilizados em ataques TDoS (Ver Figura 10). Conforme mencionado acima, os ataques TDoS são conduzidos virtualmente. Esta é uma evolução do método padrão de utilização de uma série de telefones infectados para ligar para o 9-1-1, o que foi o caso no manual de ataque TDoS de 2016 orquestrado por um adolescente do Arizona.6 A dependência dos ataques virtuais TDoS se desenvolveu devido à prevalência da tecnologia VoIP (Voice-over-IP), que permite aos indivíduos enviar um número arbitrário de "ligações telefônicas", sem primeiro ter que obter acesso a uma ampla gama de telefones. Avaliamos anteriormente que era provável que estes ataques TDoS virtuais tivessem origem na atividade de botnet, especificamente máquinas com capacidades VoIP vendidas na dark web ou em fóruns criminosos.

Foram observados vários membros vendendo serviços de "inundação telefônica" em fóruns clandestinos, com preços baixos de apenas $3 USD por hora. Estes serviços de inundação incluíam chamadas telefônicas virtuais e capacidades de inundação por SMS, com um usuário descrevendo-o como um ataque de de Distributed-Denial-of-Service (DDoS) para telefones. Embora não houvesse nenhum caso de metas de segurança pública ou tecnologias mencionadas em associação com estes serviços de inundação, acreditamos com alta confiança que estes recursos poderiam ser usados contra PSAPs - especificamente contra sistemas de recebimento e tratamento de chamadas. É provável que serviços de inundação de chamadas como estes sejam utilizados por muitos dos indivíduos ou grupos por trás dos ataques TDoS.

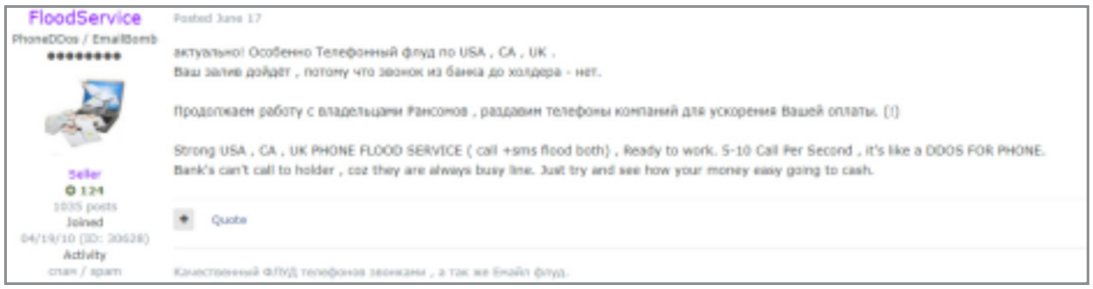


FIGURA 10: Usuário do fórum clandestino 'FloodService' vendendo chamadas e SMS de inundação.

DEFESAS RECOMENDADAS

A natureza interconectada dos PSAPs, tanto com serviços de atendimento/tratamento de chamadas quanto com redes CAD, exige que os projetistas de produtos implementem uma abordagem de segurança em camadas, aplicada e abrangente. VPNs de entrada; conexões com redes municipais adjacentes; contas de domínio amplamente utilizadas; e ocasionalmente estações de trabalho habilitadas para Internet, são todos riscos potenciais de segurança que poderiam facilitar um ataque contra OS sistemas CAD dentro dos PSAPs. Enquanto isso, os ataques TDoS não podem ser defendidos de forma confiável. A criação de opções de backup para quando o 9-1-1 ou chamadas de emergência são interrompidas pode ajudar a dar aos cidadãos a chance de ainda interagir com os operadores de chamadas durante as emergências. O lançamento de linhas telefônicas não emergenciais em sites de mídia social tem sido até agora a tática mais comum utilizada pelos defensores enquanto no meio de ataques TDoS. No entanto, essas linhas telefônicas também podem ser alvo de ataques TDoS, portanto o reencaminhamento de chamadas para os condados próximos é uma prática comum.

A implementação do MFA, quando aplicável e apropriado, pode servir para limitar o perigo de credenciais VPN comprometidas. As recentes ordens executivas nos Estados Unidos impulsionaram a modernização e implementação de padrões mais fortes de segurança cibernética através de uma arquitetura de confiança zero. Essas ordens incluíam um mandato para que o MFA garantisse que os sistemas federais estivessem protegidos contra as crescentes ameaças de ransomware.

Qualquer permissão para estações de trabalho conectadas à Internet dentro das redes PSAP deve ser documentada, pois as estações de trabalho conectadas à Internet representam um risco e são um provável vetor de infecções por ransonware.

Finalmente, como mencionado acima, uma das perturbações mais comuns dos PSAPs ocorre quando uma rede municipal adjacente ou "espinha dorsal" é desativada como resultado de uma infecção de ransomware. Nesses casos, mesmo quando a rede PSAP em si não está diretamente comprometida, pode ocorrer uma degradação dos serviços ou até mesmo interrupções.
Como tal, os centros de comunicação devem esperar que os ataques de extorsão às redes municipais tenham uma chance significativa de impactar também as funções de CAD ou do 9-1-1 de atendimento/ atendimento de chamadas.

VIGILÂNCIA POR VÍDEO

VÍDEO FIXO

ESTADO ATUAL DE CÂMERAS E NOVOS RISCOS DE SEGURANÇA

O desenvolvimento da tecnologia de vídeo fixo permite o monitoramento sofisticado e o alerta de atividades irregulares ou maliciosas em ambientes físicos. Para realizar a última geração de vigilância por vídeo, as soluções de vídeo fixo migraram de câmeras analógicas para câmeras baseadas em IP. Isto cria um novo e significativo vetor de ameaça que aumenta a superfície de ameaça para sistemas anteriormente isolados.

Muitos clientes de soluções de vídeo fixo podem não compreender completamente o aumento das ameaças como resultado desta transição. Isto resultou em um grande número de sistemas de vigilância fixos que ficaram sem controle, sem monitoramento e sem segurança.

De um milhão de câmeras expostas e 125.000 servidores expostos identificados por Shodan, 90% foram expostos sobre HTTP, 8% sobre telnet, 8% sobre SSH e 3% sobre MySQL. Estes tipos de exposições poderiam permitir que invasores remotos tivessem acesso a redes de vigilância, facilitando operações criminosas devido a vulnerabilidades conhecidas, não corrigidas ou ainda por descobrir nos protocolos ou nos próprios produtos.[7]

Além disso, novos sistemas de câmera baseados em IP estão sendo integrados em ofertas de nuvens, permitindo acesso remoto, visualização e controle de redes de câmeras. O acesso adicional à nuvem aumenta a oportunidade de configuração errada ou de contas e chaves expostas que poderiam permitir que a entidade de ameaça tenham acesso a conjuntos completos de clientes ou a redes de câmeras individuais. Por exemplo, em 9 de março de 2021, o grupo de hackers "APT69420", também referido em fontes públicas como "Arson Cats", descobriu as credenciais hardcoded para uma conta do super administrador Verkada na infra-estrutura DevOps exposta à Internet.

Todo e qualquer ambiente DevOps exposto à Internet poderia resultar em uma falha crítica de segurança que ameaçasse fortemente os agentes alvo em seu reconhecimento, pois, na maioria das vezes, credenciais e chaves de acesso sensíveis são codificadas ou expostas como resultado de práticas inseguras. Auditorias adequadas e frequentes e políticas de segurança aplicadas são essenciais para que as equipes de desenvolvimento inibam qualquer exposição não intencional. No incidente Verkada, as contas "superadministrador" codificadas no ambiente DevOps exposto permitiram que as entidade da ameaça visualizassem todas as filmagens de vigilância do cliente que tiveram como suporte o serviço de nuvem.[8]

PANORAMA DE AMEAÇAS

Confiamos de forma moderada de que aos agentes de ameaça que mais provavelmente visualizarão a vigilância por vídeo fixo não são muito sofisticados. Isto inclui hacktivistas ideologicamente motivados, operadores de botnet ou de criptografia de mining e kiddies de script com motivação notória.9 Baseamos esta avaliação nos TTPs usados pelos agentes em compromissos observados, bem como na baixa prevalência de dados valiosos em sistemas de vídeo fixo quando comparados a outras tecnologias de segurança pública.

É improvável, mas possível, que as redes de câmeras IP também possam ser alvo de ameaças mais sofisticadas para facilitar a atividade criminosa ou de espionagem em redes empresariais adjacentes, mas provavelmente exigiria implantações de sistemas mal configurados conectados a redes empresariais adjacentes ou à Internet aberta. Os sistemas fixos de vigilância por vídeo são avaliados com confiança moderada para representar um valor financeiro mínimo para os agentes de ameaça sofisticados.

Os sistemas de vídeo fixo são geralmente implantados em escolas, estádios, locais de fabricação e locais governamentais. Os dados armazenados por esses sistemas raramente são vitais para as funções cotidianas dessas organizações. Portanto, é pouco provável que o vídeo fixo seja direcionado propositalmente por grupos de crimes eletrônicos realizados. Da mesma forma, os dados de vídeo fixo raramente contêm inteligência valiosa e não representam um alvo provável para campanhas de espionagem. Como tal, não foram observados ou identificados grupos de ameaça proeminentes ou conhecidos por serem sofisticados, visando sistemas de vídeo fixo. Entretanto, como manter e proteger a privacidade dos que estão sendo monitorados, como no caso das escolas, proteger os ativos de segurança em vídeo é essencial para garantir que as transmissões de vídeo não possam ser expostas.
A ameaça mais frequente contra sistemas fixos de vigilância por vídeo é a absorção em botnets, resultando em uma possível degradação do serviço. Em 12 de outubro de 2016, a rede de bots Mirai escaneou a Internet aberta para as portas Telnet.[10]

O botnet então impulsionou uma combinação de 61 combinações de nomes de usuários/senhas geralmente usadas como credenciais padrão em dispositivos de Internet das coisas (IoT), para tentar entrar em sistemas identificados. Nesses sistemas IoT estavam incluídas câmeras de vídeo IP fixas.

Após infectar as câmeras IP e outros dispositivos IoT, a rede de botnets Mirai lançou um ataque em larga escala de Distributed-Denial-of-Service (DDoS) contra a organização de infra-estrutura DNS Dyn, interrompendo os serviços de Internet para a costa leste dos Estados Unidos. No pico da rede de botnets, houve cerca de 600.000 casos simultâneos de dispositivos IoT infectados.[11]

Desde 2016, o botnet IRCTelnet comprometeu as câmeras IP sobre Telnet através de tentativas de força bruta e credenciais padrão de forma semelhante a Mirai, embora em menor extensão.[12]

Os botnets visam dispositivos IoT para inclusão em ataques DDoS como o Mirai, mas também para o mining de moedas criptográficas. Outros indivíduos demonstraram interesse em obter acesso a sistemas de vídeo fixo e Avigilon, (ver Figura A abaixo). É mais provável que isto facilite o acompanhamento de comportamentos como a criação ou ampliação de um botnet e a exposição de dados de vídeo, mas também pode permitir a atividade de extorsão em raras instâncias. O comportamento acima é representado pelos seguintes TTPs: Serviços Remotos, Contas Padrão, Adivinhação de Senha, Sequestro de Recursos e Network Denial od Service.[13]

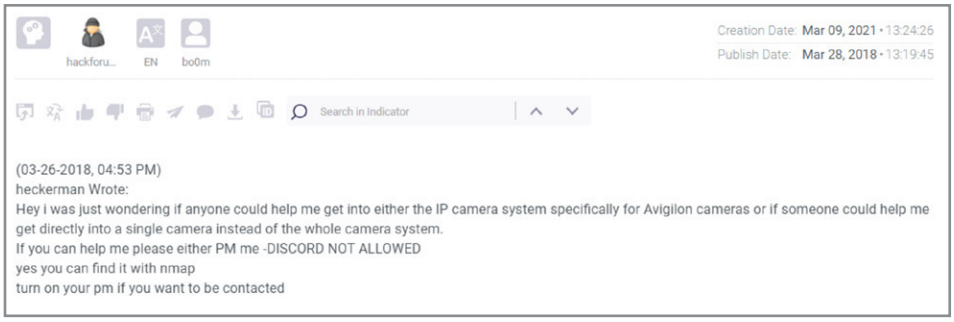


IMAGEN A: El usuario "heckerman" preguntando sobre cómo obtener acceso al sistema de cámaras IP de Avigilon.

Em 9 de março de 2021, os agentes de ameaça tiveram acesso à empresa de câmeras de vigilância gerenciada Verkada e tiveram acesso a 150.000 câmeras ao vivo instaladas em toda a sua base de clientes. Os agentes de ameaça supostamente ganharam acesso aos sistemas de vigilância usando uma conta descoberta de super administração da Verkada na infraestrutura DevOps que foi exposta à internet. A partir daí, os agentes de ameaça conseguiram capturar imagens de tela e acessar imagens de vídeo ao vivo e vídeos arquivados. É avaliado com confiança moderada que os invasores só tiveram acesso aos feeds das câmeras sendo gerenciados pela oferta da Verkada na nuvem. Isto é baseado em alguns dos clientes da Verkada que confirmaram que nenhum de seus sistemas de armazenamento de vídeo no local foi comprometido no ataque e que somente as câmeras conectadas aos serviços de nuvem da Verkada foram expostas. Outros clientes da Verkada afetados incluem a prisão do Condado de Madison em Huntsville, Alabama; o centro de detenção do Condado de Graham, no Arizona; e uma delegacia de polícia sem nome em Stoughton, Massachusetts. Os TTPs identificados no hack estavam incluídos: Contas Válidas, Captura de Vídeo e Captura de Áudio.

Os sistemas fixos de vigilância por vídeo podem ser direcionados como parte de outras operações de acesso. Em 17 de janeiro de 2017, dois indivíduos romenos de baixa sofisticação comprometeram as câmeras do Departamento de Polícia Metropolitana de Washington, D.C. em um esquema de ransomware mal sucedido.14 Isto resultou em uma perda de quatro dias de disponibilidade para as câmeras, pois elas foram tiradas do ar durante os esforços de remediação. Os agentes visaram as câmeras de vigilância com a intenção de usá-las como uma base para as redes adjacentes e usaram o RDP para se mover lateralmente de câmeras comprometidas para 123 computadores conectados.

Os agentes de ameaça cometeram vários erros, incluindo a opção de enviar ransomwares via 179.00 emails individuais, usando um serviço de email em massa, em vez de comprometer um controlador de domínio e executar ransomwares a partir daquela posição elevada.15 Os agentes também demonstraram baixa segurança operacional ao usar uma conta Gmail com um dos nomes do operador como endereço de recuperação para uma conta separada que estava ligada ao ataque, demonstrando sua falta de sofisticação. O método inicial de acesso no compromisso de Washington, D.C. não é relatado. Embora a tentativa não tenha sido bem sucedida, serve como exemplo de como as redes de câmeras por IP podem ser apenas o alvo inicial dos invasores em casos incomuns.

DEFESAS ATUAIS E RECOMENTADAS

Os invasores mais propensos a visar soluções de vídeo fixo são provavelmente de baixa sofisticação. Portanto, garantir que os controles de segurança fundamentais sejam aplicados no nível do produto, assim como garantir que os fornecedores terceirizados estejam utilizando as melhores práticas quando trabalham com seus clientes pode ajudar a inibir e impedir a maioria dos ataques.

Câmeras de vigilância fixas bem seguras devem ser expedidas em senhas padrão. Elas também devem ter o firmware assinado e criptografado. Deforma ideal, cada família de câmeras deveria ter uma chave de criptografia única e derivada, que pode ser revogada à vontade. Além disso, as câmeras devem ser enviadas com cartões de criptografia embarcados para mitigar os impactos do roubo e da adulteração. Os usuários finais, entretanto, devem assegurar-se de que estão fazendo o patch e atualizando suas câmeras a partir de uma fonte designada oferecida por seu fornecedor, para garantir que eles não sejam expostos a quaisquer vulnerabilidades e explorações conhecidas, o que poderia contornar os controles de segurança.

No final, uma segurança consistente e completa recai sobre os usuários finais. Por exemplo, mesmo quando um produto em si é protegido, se não houver nenhum comprimento de senha ou exigência de complexidade para acessá-lo, a barreira de acesso é significativamente reduzida devido ao risco de exposição ou vazamento de credenciais. A concepção errada em torno da conectividade das câmeras IP com a Internet resultou em um número significativo de usuários finais falhando em colocar o patch em suas câmeras, pois eles normalmente não classificam as câmeras como parte de seus sistemas OT. Embora muitas câmeras sejam seguras por si mesmas, elas requerem gerenciamento e instalação eficazes, além de soluções de monitoramento sustentado e abrangente.

Com base em eventos como o hack Verkada, é fundamental que os sistemas de câmeras IP, ambientes de nuvem e ambientes de desenvolvimento estejam isolados da Internet aberta. Não há nenhuma razão legítima conhecida para que uma rede de câmeras IP permita o tráfego Telnet ou HTTP para sistemas desprotegidos, não monitorados e não autorizados. Os vendedores terceirizados devem ser avaliados quanto às melhores práticas de segurança demonstradas. Isto ajudará a garantir que aqueles que ajudam os clientes de câmeras a instalar e configurar produtos de câmeras de vigilância sejam capazes e dispostos a usar as melhores práticas seguras para proteger a missão de seus clientes.

Os ataques históricos de serviços de vídeo destacaram a importância do controle de acesso. O acesso de fornecedores deve ser limitado somente quando o cliente o permite e somente para sessões individuais. Além disso, recomenda-se que auditorias e testes de penetração sejam realizados regularmente e que o acesso concedido seja cuidadosamente monitorado para garantir que este continue sendo o caso.

Além de separar as redes de câmeras IP e os ambientes de nuvem dos sistemas abertos de Internet, eles também devem ser isolados das redes empresariais adjacentes, incluindo os ambientes DevOps. No momento da implantação, limitar o acesso de e para as redes de vídeo é a melhor prática que deve ser compartilhada através da documentação do produto com possíveis vendedores terceirizados. Isto pode ajudar a mitigar potenciais compromissos em larga escala caso as redes de câmeras IP sejam usadas para obter acesso oportunista a redes organizacionais ou de consumo maiores.

LEITORES DE PLACAS DE CARRO (LPR)

DIRECIONAMENTO ANTERIOR E COMPROMETIMENTO DE SISTEMAS E DADOS DE LPR

Identificamos quatro incidentes que impactaram o espaço do leitor de placas (LPR) desde 2015, além da identificação de sistemas LPR vulneráveis e expostos através das varreduras Shodan. A maioria desses casos envolveu dispositivos, bancos de dados e/ou portais da Web que eram acessíveis abertamente pela Internet, sem necessidade de autenticação. Um dos quatro incidentes ocorreu em abril de 2020.16 Nossa equipe descobriu apenas um caso de uma entidade ameaçadora que comprometia um negócio da LPR: um ataque de ransomware contra Perceptics em maio de 2019. O grupo de extorsão Team Snatch comprometeu a Perceptics no que foi um dos primeiros exemplos de grupos de extorsão usando tanto o ransomware como o roubo de dados como tática e exfiltrou 449 gigabytes de dados da empresa.

Isto incluiu arquivos de propriedade de um dos clientes da Perceptic, a agência de Alfândega e Proteção de Fronteiras dos EUA. Os dados roubados incluíam fotos de rostos e licenças de mais de 100.000 viajantes entrando e saindo dos Estados Unidos. Não sabemos qual método(s) o invasor usou para obter acesso à rede da Perceptic. Não há indicação de que a violação tenha sido devido a uma vulnerabilidade na própria pilha de tecnologia LPR ou que o ataque tenha sido motivado pelo envolvimento da empresa no negócio da LPR. Depois que a Perceptics não pagou o pedido de resgate, a equipe Snatch forneceu os arquivos roubados aos moderadores do site de fuga hacktivista, DDoSecrets. Os moderadores do DDoSecrets então publicaram os dados do Perceptics em junho de 2019. O ataque resultou na proibição pelo CBP do uso do Perceptics dentro da organização e por contratantes federais.[17]

CRIMINOSOS CIBERNÉTICOS

Vender informações financeiras pessoalmente identificáveis roubadas de redes comprometidas, computadores individuais infectados, bancos de dados vazados ou ataques de phishing, continua sendo uma das maiores prioridades dos cibercriminosos.

Durante o ano passado, nossa equipe encontrou discussões mínimas dentro do subterrâneo criminoso em relação à tecnologia LPR, empresas ou outros produtos LPR. Nossa investigação na dark web e em fontes abertas não identificou nenhum fórum ou grupo criminoso dedicado focado em intrusões da LPR ou no uso indevido de dados de placas derivados de dados registrados da LPR. Não encontramos discussões sobre ataques diretos planejados a empresas cujas operações comerciais principais giram em torno da criação ou manutenção da tecnologia LPR em fóruns da dark web.

Em vez disso, identificamos uma tendência de agentes clandestinos dispostos a compartilhar links para relatórios de código aberto ou recursos para ajudar a identificar dispositivos LPR vulneráveis ou dispositivos IoT, particularmente em repositórios de código como o GitHub.[18]

A maioria das referências a empresas que fornecem produtos LPR apareceu em mercados clandestinos proeminentes, tais como Genesis Store, Russian Market ou Amigos Market, mas provavelmente estavam afiliadas ao compromisso de contas de consumidores, ao invés de contas administrativas. Além disso, fóruns clandestinos e serviços de mensagens estão sendo amplamente utilizados por participantes interessados em componentes mais técnicos dentro da tecnologia IoT, especificamente sistemas de câmeras CCTV, em vez de produtos ou dados LPR, indicando uma falta de valor financeiro disponível nas tecnologias LPR e dados para criminosos cibernéticos.

Não identificamos referências específicas ao mau uso criminoso da tecnologia LPR. Ao contrário, a inteligência que está sendo compartilhada e discutida poderia ser usada por uma entidade de ameaças para adquirir conhecimento sobre componentes técnicos, bem como aprender as melhores práticas com outros participantes

> Discussões sobre ataques diretos planejados a empresas cujas principais operações comerciais giram em torno da criação ou manutenção da tecnologia LPR não foram descobertas em fóruns da dark web.

HACKTIVISTAS

A LPR continua sendo uma tecnologia controversa, com críticos afirmando que eles representam uma vigilância cada vez mais difundida e intrusão na privacidade.19 Julgamos que isto pode motivar os agentes hacktivistas a atacar os sistemas LPR, com o objetivo de gerar publicidade e expor sistemas inseguros. É provável que os fornecedores e usuários da LPR representem um alvo para os agentes de ameaça hacktivista politicamente motivados por razões similares à violação da Verkada: atacar contra a percepção de excesso de confiança na vigilância pública. No entanto, não obtivemos nenhuma inteligência específica sobre a intenção atual de atacar os sistemas LPR.

Examinamos fóruns de código aberto, serviços de mensagens e websites relacionados à segurança para conteúdo relacionado à tecnologia LPR, assim como fornecedores ou produtos LPR. Em nossa investigação, identificamos diversos fóruns, para marcas específicas, onde os usuários

discutiram os tópicos acima, mas não identificamos conteúdo que consideramos malicioso que esteja relacionado à exploração da LPR ou ao direcionamento de qualquer um dos sistemas acima mencionados. A análise de uma amostra de tópicos do fórum identificou os seguintes temas:

- Eles não identificaram usuários discutindo vulnerabilidades dentro de componentes LPR, especificamente em software que poderia ser usado para fins maliciosos.
- Conversas sobre LPR, tanto sobre o básico da tecnologia quanto sobre como ela supostamente agrava o problema percebido de vigilância excessiva.

Nossa equipe observou uma diminuição na atividade hacktivista internacional em geral, à medida que o cenário hacktivista se afastou de uma ampla participação pública e voltou para suas origens como prática de grupos menores de indivíduos dedicados. Como tal, os ataques relacionados ao hacktivismo geralmente resultaram em um dos seguintes efeitos:

- Denial-of-service
- Defacement de sites e portais de face pública
- Exposição pública de dados sensíveis

ESTADOS-NAÇÃO

Não descobrimos nenhum caso específico de agentes de ameaça patrocinados pelo estado que procuravam acessar secretamente sistemas LPR ou dados gerados pelo LPR. Julgamos que pelo menos alguns grupos patrocinados pelo Estado teriam interesse em obter tais dados para fins de inteligência, por exemplo, para rastrear os movimentos de indivíduos estrangeiros de interesse. No entanto, em geral, avaliamos que isto provavelmente não seria considerado um conjunto de dados de alta prioridade a serem obtidos.

VULNERABILIDADES COMUNS E MÉTODOS DE INFECÇÃO

As câmeras de leitura de placas de carro ficam sob o guarda-chuva dos dispositivos IoT. Esses dispositivos são geralmente direcionados e comprometidos com o propósito de criar um botnet, muitas vezes através do uso excessivo de credenciais padrão ou da ameaça de agentes que forçam senhas fracas. Estes botnets são frequentemente usados para realizar ataques DDoS. Entretanto, a maioria dos comprometimentos observados com os próprios sistemas LPR foram simplesmente o resultado da falta de autenticação das redes expostas de provedores de serviços.

Um tema que nossa equipe identificou dentro da clandestinidade criminosa foi o interesse entre os agentes em compartilhar pesquisas ou técnicas para identificar tecnologias de Internet sem fio vulneráveis, capazes de serem exploradas. Entretanto, as menções à tecnologia LPR em associação com essas consultas ainda eram mínimas.

Descobrimos uma instância de vulnerabilidades descobertas especificamente em relação às câmeras LPR. Em 21 de janeiro de 2021, um pesquisador da empresa macedônia Zero Science Lab publicou detalhes de nove vulnerabilidades que afetam vários modelos de câmeras LPR vendidas pela Selea, uma designer e fabricante italiana.A Selea parece ser uma empresa relativamente pequena sem uma grande participação no mercado. As vulnerabilidades foram posteriormente publicadas em vários sites de repositório de vulnerabilidades e exploração, tais como exploit-db.

As nove vulnerabilidades incluíam uma vulnerabilidade de travessia de diretório não autenticada que permitiria que um invasor recuperasse credenciais e uma vulnerabilidade de injeção de comando remoto pós- autenticação.

Estas duas vulnerabilidades poderiam ser facilmente encadeadas para permitir a execução de código remoto não autenticado. Houve apenas uma menção a estas vulnerabilidades encontradas na dark web ou em fóruns clandestinos e não há mais nenhum contexto em torno desta referência para indicar se houve algum interesse significativo. Não descobrimos nenhuma indicação de que estas vulnerabilidades tivessem sido ou estejam sendo exploradas ativamente.

PERSPECTIVA FUTURA DA INDÚSTRIA LPR

É provável que veremos outros casos de dados LPR inadequadamente protegidos, incluindo dispositivos ou portais de acesso que estejam abertamente acessíveis através da Internet.

Assim como a Perceptics, as empresas LPR podem se tornar alvos de campanhas de ransomware, embora não acreditemos que seja especificamente seu envolvimento na tecnologia LPR que permita ou motive tais ataques.

Devido à natureza controversa dos aspectos da tecnologia, a tecnologia LPR continuará a representar um alvo potencial para os agentes de ameaça hacktivista.
Embora tenha havido inteligência limitada encontrada na dark web e nos fóruns da clearnet em relação aos ciberataques planejados e à exploração da vulnerabilidade na tecnologia LPR, julgamos que os fóruns

continuarão, muito provavelmente, a atrair agentes de ameaça interessados na tecnologia IoT e nos avanços tecnológicos da indústria.

EQUIPADOS COM INSIGHT

ENFRENTANDO COM CONFIANÇA OS DESAFIOS CIBERNÉTICOS DE HOJE

À medida que nos aproximamos do segundo ano da pandemia da COVID-19, os sistemas e os dados de segurança pública estão se tornando cada vez mais integrados, criando novos desafios para as equipes de segurança que se defendem contra criminosos, estados-nação, hacktivistas e outros.

Estes maus agentes sabem que serviços de emergência confiáveis e seguros são essenciais para combater a pandemia e manter os cidadãos a salvo de outros perigos cotidianos. Isso é o que os torna alvos tão aliciantes.

Nossa esperança é que o conhecimento contido neste relatório permita que as organizações de segurança pública lutem com uma visão acionável sobre os métodos, objetivos e operações dos adversários.
Hoje, este conhecimento é um elemento central de cada produto e serviço que a Motorola Solutions oferece. Nossos clientes enfrentam ameaças cibernéticas cada vez mais sofisticadas e perigosas.

No entanto, eles não estão enfrentando esta ameaça sozinhos. Equipados com insights como os encontrados no relatório Soluções Cibernéticas de Ameaças à Segurança Pública 2021 da Motorola Solutions, eles podem enfrentar com confiança os desafios cibernéticos atuais.

GLOSSÁRIO DE TERMOS

TÁTICAS, TÉCNICAS E PROCEDIMENTOS QUE NÃO ESTÃO NA ESTRUTURA DE MITRE ATT&CK:

- **Linhas administrativas:** Números de telefone de entrada específicos pertencentes aos PSAPs (tais como números 1-800). Estas linhas existem além das linhas de emergência utilizadas para o roteamento de chamadas 9-1-1.
- **9-1-1 Direto:** Os agentes de ameaças podem ligar diretamente para linhas de emergência (como 9-1-1 nos Estados Unidos) para alvejar PSAPs locais em ataques de Negação de Serviço de Telefonia.
- **Extorsão de Dados / Publicação:** Os agentes de ameaça podem roubar dados com o objetivo de extorquir vítimas para sua liberação. Nesses casos, os agentes de ameaça podem publicar partes dos dados em sites personalizados e de compartilhamento de dados. Este comportamento é frequentemente observado em associação com grupos de extorsão.
- **Hardware ou Roubo de Chaves:** Uma forma comum para os agentes de ameaça obterem acesso às transmissões LMR. Os agentes de ameaças podem usar rádios roubados ou chaves de criptografia de hardware para vigiar as comunicações criptografadas entre os socorristas e os oficiais federais. Os agentes de ameaça também podem usar rádios roubados ou chaves de criptografia de hardware para conduzir ataques de Negação de Serviço de Radiodifusão.
- **Acesso Inerente:** Os infiltrados maliciosos ou inadvertidos são um fator comum nos comprometimentos dos sistemas ou transmissões LMR. O Acesso Inerente é o termo usado para descrever ataques ou eventos nos quais nenhuma ação externa foi necessária para obter acesso ao LMR.
- **Negação de Serviço de Radiodifusão:** Os agentes de ameaça podem perturbar as comunicações da LMR por motivos políticos, ideológicos ou financeiros, transmitindo sons e informações falsas, confusas ou arbitrárias através de canais de conversação criptografados e não criptografados. Esta tática é frequentemente usada em conjunto com Hardware ou Roubo de Chave, especialmente nos casos em que as comunicações de canais criptografados são interrompidas.
- **Telephony Denial of Service [Negação de Serviço Telefônico]:** Um ataque de Telephony Denial of Service (TDoS) é uma tentativa de tornar um sistema telefônico indisponível para os usuários pretendidos, impedindo a entrada e/ou saída de chamadas. Isto é conseguido quando os agentes de ameaça consomem de forma bem sucedida todos os recursos telefônicos disponíveis, de modo que não há uma linha telefônica desocupada.

NÍVEIS DE CONFIANÇA ANALÍTICA

- **Alta Confiança**: Geralmente indica julgamentos baseados em informações de alta qualidade e/ou a natureza da questão torna possível fazer um julgamento sólido. Um julgamento de "alta confiança" não é um fato ou uma certeza, entretanto, e ainda carrega o risco de estar errado.
- **Confiança Moderada:** Geralmente significa informação credível e plausível, mas não de qualidade ou corroboração suficiente para garantir um nível mais alto de confiança.
- **Baixa Confiança:** Geralmente significa que foram usadas informações questionáveis ou implausíveis, as informações são muito fragmentadas ou pouco corroboradas para fazer inferências analíticas sólidas, ou que existem preocupações ou problemas significativos com as fontes

FONTES

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 Security of IP-Based Video Surveillance Systems." Sensors (Basel, Switzerland) vol. 20,17 4806.August 26th. 2020, doi:10.3390/s20174806 8 https://www.bleepingcomputer.com/news/security/hackers-access-surveillance-cameras-at-tesla-cloudflare-banks-more/

9 Alguém que não tem conhecimento de rede e programação, e que usa o software existente para lançar um ataque. Muitas vezes, um kiddie de script usa esses programas sem saber como eles funcionam ou o que fazem.

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 Ver attack.mitre.org para mais detalhes.

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 Um sistema de dispositivos computacionais interrelacionados, máquinas mecânicas e digitais, objetos, animais ou pessoas que são fornecidos com identificadores únicos e a capacidade de transferir dados através de uma rede sem a necessidade de interação de humano para humano ou de humano para computador.

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

Para mais informações sobre nossos Seriços de Cibersegurança, entre em contato com seu representante Motorola Solutions ou 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 e o logotipo M estilizado são marcas comerciais ou marcas registradas da Motorola Trademark Holdings, LLC e são utilizados sob licença.
Todas as outras marcas registradas são de propriedade de seus respectivos proprietários. © 2021 Motorola Solutions, Inc. Todos os direitos reservados. 10-2021