2020 CYBER THREATS TO PUBLIC SAFETY

ATTACK METHODS TARGETING EMERGENCY SERVICES

MOTOROLA SOLUTIONS

For almost a century, Motorola Solutions has pioneered groundbreaking public safety solutions for law enforcement, fire, EMS, 9-1-1 and other state and federal agencies. Today, we continue to build leading emergency services technology while also helping customers manage their cybersecurity awareness, protection, detection, response and recovery efforts. This dual position as both a public safety and cybersecurity solutions provider provides unique insight into the established and emerging cyber threats facing emergency services.

The Motorola Solutions Threat Intelligence Team built on our 2019 cybersecurity report, identifying the most significant threats and threat actors targeting public safety in 2020. To that end, we conducted in-depth research throughout the year, using anonymized closed-sourced data from Motorola Solutions platforms from January 1 through September 23, 2020, along with publicly reported information and expert analysis.

Our findings focus specifically on current cyber threats to public safety, including public safety communication, public safety answering points, body worn cameras, evidence storage and the overall technology ecosystem. This report does not cover commercial radio and fixed video technologies.

We hope you find the Motorola Solutions 2020 Cyber Threats to Public Safety report informative. As part of our continuous efforts to improve the public safety cybersecurity toolkit, we believe our findings can empower public safety leaders and practitioners as you work to make emergency services more secure in 2020 and beyond.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The public safety officer's toolkit has undergone a significant evolution from even a few years ago. Today, every system is being connected to IP-based networks and to each other. This connectivity extends from the radios used to communicate in the field, to the public safety answering points receiving emergency calls and dispatching the proper units, to video evidence gathering and storage systems. Yet, the added benefits of interconnectivity and easier access come with inherent security risks. New public safety technology must be approached in the same manner as traditional IT equipment, with proper patch management and monitoring, rather than the "set and forget" method that worked in previous, non-connected public safety equipment.

In 2020, malicious actors increased their activity and sophistication to execute continuous, successful cyber campaigns which exploited fear surrounding the COVID-19 pandemic and recent civil unrest. Public safety organizations, however, have seen an overall 44% decrease in cyber attacks (88 attacks total) compared to the previous year (158 attacks). Financially motivated eCrime gangs shifted their focus to other industries, while hacktivist activity increased as a result of civil unrest.

Public Safety Answering Points (PSAP), which are critical for routing emergency calls, continued to be the most frequently targeted location in public safety, most commonly with low impact Telephony Denial-of-Service (TDoS) attacks. Records and Evidence (R&E) storage were the most frequent systems to be severely impacted by cyber attacks in 2020. Land Mobile Radio (LMR) communication systems saw very few instances of compromise in 2020, but a need for threat hunting has been identified to ensure no Advanced Persistent Threat (APT) or malicious activity exists in any public safety LMR cores.

External Remote Services, such as Remote Desktop Protocol (RDP), continued to be the most common infection method for threat actors targeting public safety, with threat actors conducting increased network reconnaissance for maximum data theft. The Motorola Solutions Threat Intelligence team compiled the Tactics, Techniques and Procedures (TTPs) mapped to the MITRE ATT&CK framework with associated threat actors who have and are assessed to continue, targeting public safety.

Levels of Analytic Confidence

- **High Confidence:** Generally indicates judgments based on high-quality information and/or the nature of the issue makes it possible to render a solid judgment. However, a "high confidence" judgment is not a fact or a certainty and still carries a risk of being wrong.
- **Moderate Confidence:** Generally means credibly sourced and plausible information, but not of sufficient quality or corroboration to warrant a higher level of confidence.

New public safety technology must be approached in the same manner as traditional IT equipment, with proper patch management and monitoring, rather than the "set and forget" method that worked in previous, non-connected public safety equipment.

Nation-state actors and cybercriminals have exploited a more vulnerable workforce, who have had difficulty rapidly shifting from walled gardens to VPN-based operations, to get initial access into their victims' networks.[1]

THE SHIFTING CYBER LANDSCAPE

In 2020, the COVID-19 pandemic significantly changed global operations at every level, in every industry. The global workforce saw a dramatic shift to remote working, creating new targets for criminal and nation-state cyber operators.

Nation-state actors and cybercriminals have exploited a more vulnerable workforce, who have had difficulty rapidly shifting from walled gardens to VPN-based operations, to get initial access into their victims' networks.[1] Overall, there have been more cyber attacks in the first half of 2020 than in all of 2019. This has been led by the eCrime industry, which is responsible for 82% of those attacks.[2]

The pandemic has also shifted the global economic forces and criticality of specific industry verticals, such as health care and manufacturing, which caused a significant target realignment for the ever-advancing eCrime threat actors. The eCrime industry successfully targeted high-value data in industries sensitive to downtime, also referred to as Big-Game-Hunting (BGH). According to a recent report, from January to June 2020, manufacturing has been the second most targeted industry in 2020, while it was not even in the top-10 most targeted industries in previous years.[3]

In 2020, the most prolific eCrime attack type was extortion. In 2019, extortion threat actors, such as Maze[4] and DoppelPaymer, relied on ransomware as the primary tool for extracting payments. However, in 2020, extortion actors also incorporated the theft of highly valuable or sensitive information into their tactics, alongside ransomware deployments. By applying further coercive measures against victims, they sought to increase the likelihood of monetary payments. At the same time, actors have also created 'data leak sites' where evidence of attacks can be posted in order to increase public awareness and external pressure on nonpaying victims.

The evolving global cyber threat landscape changed the frequency of attacks facing public safety. Threats have decreased overall while attacker profiles and motivations have shifted.

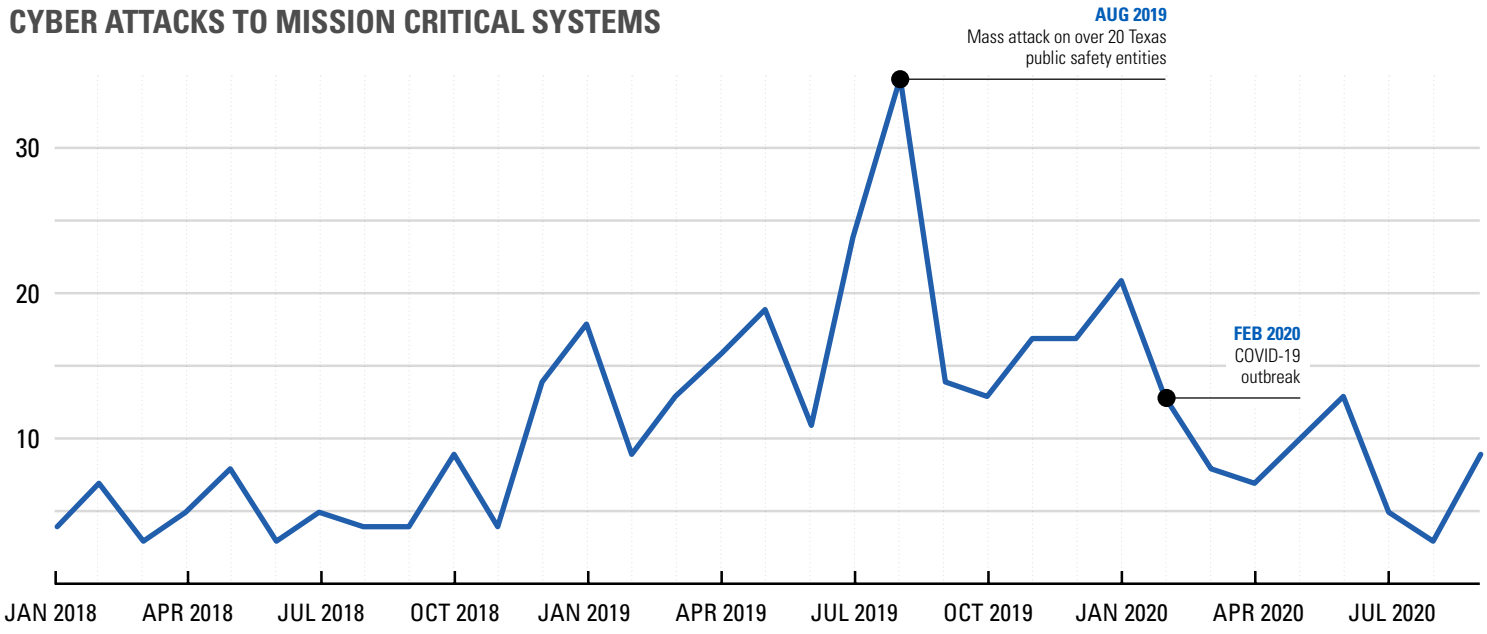


Figure 1: Publicly reported cyber attacks impacting emergency services collected and analyzed by the Motorola Solutions Threat Intelligence Team.

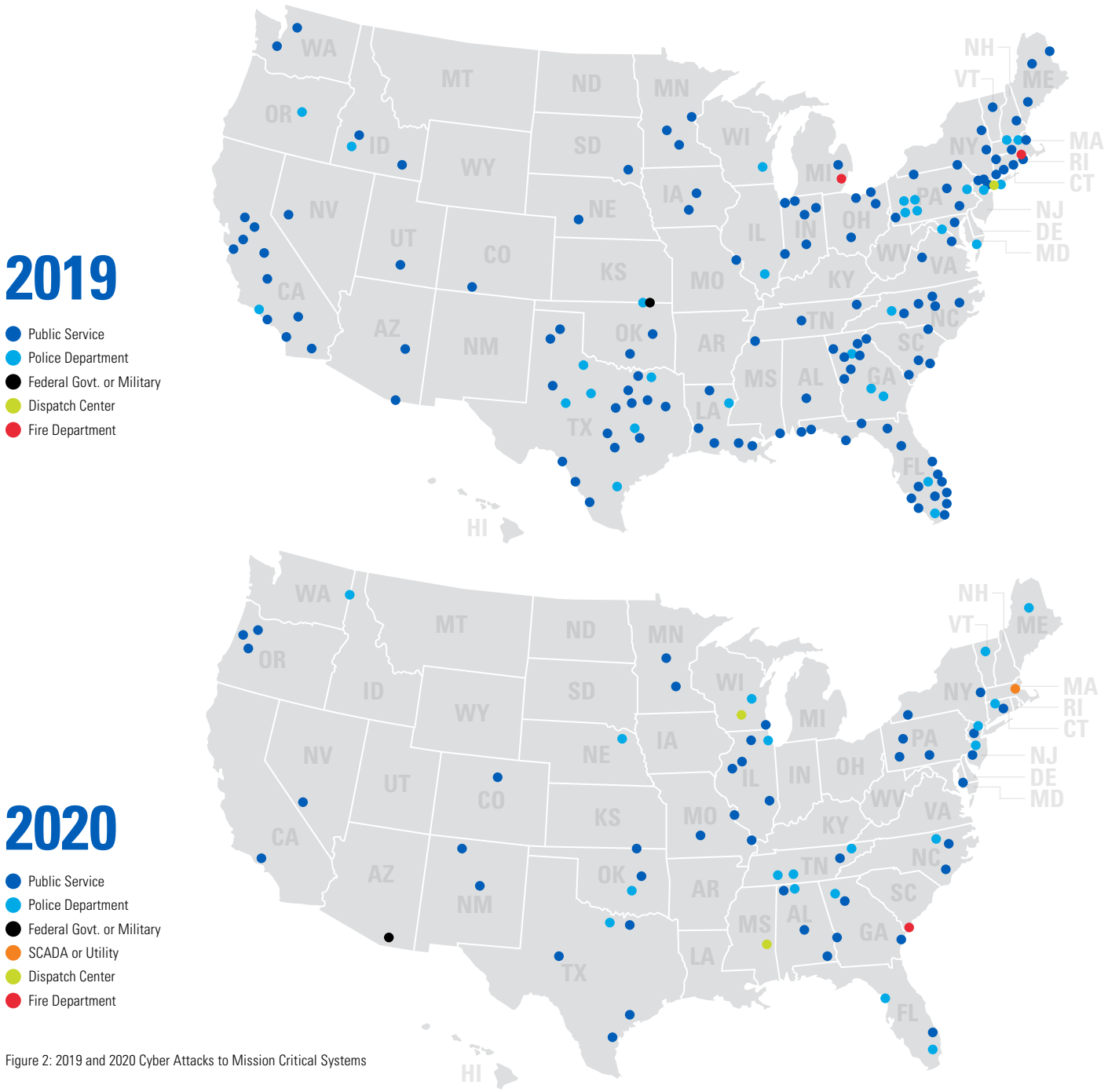


Figure 2: 2019 and 2020 Cyber Attacks to Mission Critical Systems

From January 1 through September 23, 2020, there were 88 reported cyber attacks impacting public safety, a 44% decrease from the same reporting period in 2019 (158 attacks). This is the result of a significant reduction of attacks beginning in February 2020 as COVID-19 began its economic and operational impact on the world. It is assessed that threat actors shifted from extortion campaigns targeting emergency services and municipalities to capitalize on larger extortion payments from now more exposed corporations and manufacturing facilities. This was the first observed decrease in trending cyber attacks to emergency services since we began reporting in September 2017.

The decrease in attacks continued as the COVID-19 pandemic spread throughout the world, until a brief resurgence of attacks from late May to late June. During this time, emergency services, particularly law enforcement, were highly targeted by hacktivist activity prompted by the civil unrest in the United States. This activity took the form of land mobile radio disruptions, website defacements and data breaches attempting to discredit police and municipal governments.

CYBER ECOSYSTEM

We assess with moderate confidence that the PSAP is the most likely location to be targeted by malicious actors across the public safety cyber ecosystem. While it's not often publicly reported, TDoS attacks represent a frequent and meaningful attack type which degrades dispatch centers' ability to serve the public, especially in emergency scenarios. While TDoS attacks typically don't directly prevent dispatch centers from supporting public safety officers, they often degrade their services due to lost resources or time spent transitioning calls to different dispatch centers.

INITIAL ACCESS	EXECUTION	DISCOVERY	LATERAL MOVEMENT	DATA COLLECTION	ATTACK IMPACT
External Remote Services (RDP, VPN, SMB)	Windows Management Instrumentation	Network Share Discovery	SMB/Windows Admin Shares	Data From Local System	Data Encrypted for Impact
Trusted Relationship	Malicious File	Domain Account Discovery	Remote Desktop Protocol	Data From Network Shared Drive	Data Extort/Publish
Spearphishing Attachment	Malicious Link	File and Directory Discovery	Lateral Tool Transfer	Email Collection	Telephony Denial of Service
Spearphishing Link	Windows Command Shell	System Network Connections Discovery	Exploitation of Remote Services	Audio Capture	Broadcast Denial of Service
Exploit Public-Facing Application	PowerShell	Domain Groups Discovery	Replication Through Removable Media	Data From Removable Media	Network Denial of Service
Inherent Access (Insider Threat)	Native API	System Information Discovery			Data Destruction
Valid Accounts	Service Execution	Security Software Discovery			Inhibit System Recovery
Hardware or Key Theft		System Service Discovery			System Shutdown/Reboot
Hardware Addition		Network Service Scanning			Service Stop
Replication Through Removable Media					Disk Structure Wipe

Figure 3: Heat map of TTPs used against public safety organizations, sorted in descending order of likelihood.

Although PSAPs are the most likely location to be targeted, records and evidence storage systems are assessed to be the most likely system to be severely impacted by cyber attacks, due to their connectivity to networks that may be insecure and frequent targeting by extortion groups. Public sector IT resources are shared primarily to save budget, but this can result in security holes or monitoring failures. Records and Evidence (R&E) storage systems are most frequently compromised from being connected to municipal networks and Customer Enterprise Networks (CEN). This is commonly the result of a lack of security controls and oversight.

Of the public safety technologies researched in this paper, Land Mobile Radio (LMR) saw the least number of reported instances of compromise or targeting by malicious actors. However, the threat intelligence team has seen minimal research from federal and academic institutions on the threats and vulnerabilities facing LMR. Although LMR has historically been an isolated technology, it is increasingly being connected to the internet and enterprise networks. The increased connectivity could give threat actors more opportunities to compromise the critical availability of LMR communication. Defensive measures such as patching, deploying anti-malware solutions and secure configuration are not enough to address the potential for APTs, which are able to discreetly hide in networks until they cause system-wide failure. Therefore, it is essential for organizations to conduct threat hunting activities in their LMR systems to ensure they continually monitor for and address malicious activity in LMR cores.

We assess with high confidence that threat actors targeting the public safety cyber ecosystem are most likely to use External Remote Services (such as RDP and SMB/Windows Admin Shares) to gain access to networks and systems. As extortion actors increasingly seek to steal data, we assess with moderate confidence that they will leverage methods like Network Share Discovery to uncover sensitive file repositories. Following this, actors are most likely to harvest data from Local Systems and Network Share Drives. Denial of availability is the most common attack impact across all public safety systems, resulting in Data Encrypted for Impact and TDoS. Organizations should conduct proactive threat hunting to confirm or deny the use of the above TTPs by malicious actors in an environment.

PUBLIC SAFETY ANSWERING POINTS

Public Safety Answering Points are call centers where emergency calls are routed. They typically have four primary communication flows: inbound 9-1-1 calls, outbound locational queries, outbound dispatch traffic and bidirectional administrative lines.

These administrative lines allow a PSAP to communicate with other PSAPs and often take the form of dedicated phone numbers, similar to 1-800 numbers. Most PSAPs consist of at least two primary subsystems: Emergency Call Handling (ECH) and Computer Aided Dispatch (CAD). ECH systems are IP- and telephony-based software used to accept, queue and answer emergency calls. CAD software is used to dispatch emergency personnel, including police, fire and emergency medical aid. Together, call handling and CAD form the operational core of PSAPs. In the PSAPs, call takers handle incoming calls while dispatch officers dispatch appropriate first response resources necessary to respond to the emergency calls handled by call takers. Dispatchers also obtain and relay pertinent information to units in the field, such as alerting police officers to dangerous situations.

CALL HANDLING

We assess with high confidence that Telephony Denial-of-Service (TDoS) attacks represent an immediate and credible threat to the availability of PSAPs via their ingress lines.

Based on observed attack data, we assess with high confidence that financially-motivated, low-sophistication cybercriminals are the most likely to conduct TDoS attacks and to extort victims' PSAPs for ransom. We base these assessments on reports from Motorola Solutions field personnel, observed attacks in the wild and discussions with Association of Public-Safety Communications Officials (APCO) members. These attacks are rarely reported, comprising just 15% of reported attacks impacting PSAPs. However, due to their simplicity, TDoS attacks are a consistent and frequent scourge of PSAP operators and thus require prioritization.

Telephony Denial-of-Service attacks come in two primary forms, automated and manual. To conduct manual attacks, threat actors acquire large numbers of disposable cell phones with prepaid services and use these phone numbers to overwhelm PSAP emergency and administrative lines with manually generated calls. In automated attacks, actors can run simple scripts to allow large numbers of computer-generated calls to flood administrative or emergency lines. Threat actors can conduct automated attacks easily and inexpensively via temporarily-rented botnets or even through use of simple workstation technology.

Less commonly observed but more detrimental TDoS attacks involve malware that's mass distributed to victims' mobile phones via phishing or social media links. The malware then causes the network of exploited phones to call emergency numbers like 9-1-1, flooding the PSAP with "real" but nonactionable communications. Such attacks, which require simple malware and often only a few lines of code, have been successful in compromising the availability of 9-1-1 centers across 12 states.[5]

Next Generation 9-1-1 (NG9-1-1) systems are more protected from TDoS attacks because they can process a significantly higher number of simultaneous calls than legacy systems. However, TDoS attacks can still impact PSAPs in meaningful ways, even with NG9-1-1 technology. In legacy systems, TDoS attacks place the call load on service provider lines. In NG9-1-1 systems, that impact is shifted toward the PSAP itself. This directly impacts call-taking staff in the form of successfully received, but fraudulent calls. These calls can be interspersed with legitimate ones. TDoS attacks cannot be meaningfully defended at the PSAP due to their position within the broader networking ecology and must be prevented from reaching the PSAP in the first place by engaging the threat as it enters the ESInet.

TDoS CATEGORY	TARGET	FREQUENCY	SMALL SITE SEVERITY	LARGE SITE SEVERITY
Manually Generated TDoS	Small Site	Uncommon (used in the past)	High	Low
Social Network TDoS	Large Site	Uncommon	Moderate	Low
Simple Automated TDoS	Small Site	Common	High	Low
Complex Automated TDoS	Small or Large Site	Uncommon (but coming)	High	High
Distributed Complex Automated TDoS	Small or Large Site	Uncommon (but coming)	High	High

Figure 4: Threat Taxonomy for Telephony Denial-of-Service Attacks.[6]

This is because it's the only place where sufficient capacity exists for constructive engagement. Simply, the only way the PSAP can avoid being impacted by these attacks is to prevent the attack from ever getting to the PSAP.

We assess with high confidence that the threat group most likely to target ECH in the United States and abroad is financially-motivated "script-kiddies". These attackers are often unaffiliated with any particular group or philosophy and are usually not very technically sophisticated.

We assess with moderate confidence that threat actors are most likely to source PSAPs' 1-800 numbers from internet searches and affiliated websites to call their administrative lines directly. In these attacks, threat actors are likely to use botnet-based methods to generate a high volume of calls to overwhelm ECH systems. In order to sustain TDoS attacks, threat actors are most likely to use call spoofing software and execute calls during times where defenders are unable to proactively respond, such as holidays and local or statewide events, including the recent protests in the United States.

VICTIM DISCOVERY	PHONE/COMPUTER ACCESS	CALL EXECUTION	PERSISTENCE	IMPACT
Admin Line Discovery	Botnet Purchase	Execution Via Botnet	Call Spoofing	Telephony Denial of Service
9-1-1 Direct	Botnet Creation	Scheduled Task/Job	Critical Timing	
	Drive-by Compromise	Exploitation for Client Execution		
	Phishing	Malicious Link		
		Malicious File		

Figure 5: Heat map of TTPs used against call taking, sorted in descending order of likelihood.

COMPUTER AIDED DISPATCH

Dispatchers, call takers and 9-1-1 operators use Computer Aided Dispatch (CAD) systems to effectively dispatch emergency personnel. They also leverage CAD systems to identify first responder location and status, in addition to recording and prioritizing incoming emergency calls.

We assess with moderate confidence that extortion attacks involving ransomware represent the most credible threat to CAD systems. In such attacks, financially motivated threat actors are most likely to use ransomware together with data theft against CAD systems to disrupt availability and confidentiality. We base the above assessment on observed attacks and common configuration flaws impacting CAD systems, as well as known attacker TTPs.

Though many go unreported, according to our internal research, 67% of reported attacks impacting PSAPs involved ransomware. Shared or connected networks, such as those between dispatch centers and municipalities or police, resulted in the majority of CAD ransomware infections. These connected networks allowed threat actors to move laterally into CAD systems or servers running CAD software after they initially infected police or municipality networks.

Improperly configured firewalls are also frequent vectors for attacks. Threat actors can take advantage of this to access CAD networks from the open web or adjacent networks. Internet-connected workstations are also a meaningful concern. In at least three observed attacks, phishing emails were the initial source of compromise for CAD networks. This indicates certain workstations within affected networks had internet access, which allowed workstations to be infected with malware.

Some of the threat groups that may target CAD systems within PSAPs in the United States and abroad include the Conti group, Maze group, Dharma group, Sodinokibi group, Netwalker group, PwndLocker actors, Pysa actors, RagnarLocker actors and DoppelPaymer actors. These actors are more likely to target networks with unpatched vulnerabilities or leaked credentials, rather than methodically targeting specific entities. We base this assessment on observed TTPs and attacks against both CAD systems and nonpublic safety victims.

We assess with moderate confidence that attackers are most likely to use External Remote Services, such as RDP or SMB/Windows Admin Shares and Trusted Relationships to gain initial access to CAD networks. Windows Management Instrumentation (WMI) is the most likely TTP to be used in the execution of ransomware payloads in CAD systems. Threat actors are most likely to use SMB/Windows Admin Shares and RDP to move laterally across CAD networks. We assess with high confidence that extortion actors are most likely to attempt to impact CAD systems via Data Encrypted for Impact and leakage of valuable data.

It's almost certain that threat actors will eventually target BWCs and their associated video evidence since they offer valuable data for extortion and manipulation or to further political or ideological causes through the selective leaking of evidence.

BODY WORN CAMERAS

Body Worn Cameras (BWC) have become an integral part of policing for good reason. BWCs act as a vital tool to improve evidence-based civil or criminal case outcomes. They enhance the safety of interactions between officers and the public. They also provide unalterable audio and visual evidence that can be critical for investigating crime, police-citizen interactions and use-of-force incidents.

The confidentiality and integrity of evidence gathered by BWCs can help ensure that investigations are conducted thoroughly and accurately, without manipulation.

There are currently no reported exploitations or indications of previous exploitations of law enforcement BWCs in the wild. To date, the only reported instances of compromised BWCs have involved video evidence not being properly protected in storage, rather than the camera itself.[7] Security researchers have demonstrated potential vulnerabilities in BWCs and theorized how a threat actor could operationalize them to track officers' locations, manipulate or delete stored BWC video footage, or even implant malware to obtain broader police network access.[8] However, there have been no such reported or observed attacks in the wild.

Still, it's almost certain that threat actors will eventually target BWCs and their associated video evidence since they offer valuable data for extortion and manipulation or to further political or ideological causes through the selective leaking of evidence. There is already a market for the sale or sharing of BWC footage on criminal forums and other sites.[9] For instance, on July 1, 2020, Twitter user "KF" (@dOtslash) revealed[10] and shared sensitive video files sourced from an unencrypted microSD card within an eBay-purchased Axon BWC. Further investigation found that the sensitive video files belonged to military police officials of Fort Huachuca, Arizona.

We assess with moderate confidence that the threat actors most likely to target BWCs are low-sophisticated, ideologically-motivated hacktivists and moderate-to-highly sophisticated extortion groups motivated by financial interests. This is based on the observed interest by low-sophistication actors and enthusiasts in obtaining and sharing videos sourced from BWCs and the frequent targeting of the larger records and evidence space by extortion groups (Figure 6). It is assessed that threat actors will most likely target video evidence in storage, rather than the body worn camera device itself, since video evidence maintains higher value for both financial and ideological causes.

Figure 6: Twitter user calling for the targeting of police BWC footage.

Compared to hacktivists, it's less likely that extortion groups will be observed seeking access to, and discussing, the exploitation of police technology such as BWCs. This is because actors sophisticated enough to exploit vulnerabilities in BWCs are more likely to demonstrate improved Operation Security (OpSec), a requirement for continual and successful extortion operations. Additionally, sophisticated threat actors are likely to avoid publicly discussing the targeting of law enforcement in order to avoid increased scrutiny and surveillance by law enforcement themselves.

RECORDS AND EVIDENCE STORAGE

Police departments store large amounts of sensitive data pertaining to investigations and routine policing as well as Personally Identifiable Information (PII). This information can be valuable to threat actors who sell or use it for further exploitation, identity theft, compromising evidence availability or integrity and espionage.

Attacks impacting Records and Evidence (R&E) storage can cause a loss of trust in the impacted police department, a financial burden in the form of victim identity monitoring, the disruption of ongoing investigations and the compromise of informants and covert operations. Attacks against R&E can also result in evidence being unusable in criminal courts[11] and allow for further, more targeted phishing campaigns.

In 2020, there were 15 observed cyber attacks against R&E, a 7% increase from the 14 attacks against R&E in 2019. Ransomware is responsible for at least 10 of the 2020 R&E attacks, likely because threat actors are increasingly using data theft as a means to extort victims in these attacks. We assess with high confidence that R&E is a particularly valuable target for extortion groups that steal data, since these groups can expect a higher likelihood of payouts from victims in instances where R&E is impacted. According to our internal research, extortion has played a part in 66% of the ransomware attacks we've seen against R&E.

All confirmed R&E systems impacted by ransomware were hosted on-prem. Four of the observed attacks impacting R&E systems since January 2020 were the result of assessed data breaches, such as the BlueLeaks data breach and did not involve ransomware. One other data breach that happened recently in Belarus did not involve R&E directly, but did impact police officers' PII. It is not included in the four data breaches against R&E mentioned above. Most 2020 public safety sector data breaches (not involving ransomware), including those impacting R&E, are assessed with high confidence to have been conducted by politically-motivated hacktivists in response to negative public sentiment against police departments in the United States and abroad. This sentiment stems, in large part, from the recent civil unrest in the United States and events such as the Belarusian election.

We assess with moderate confidence that threat actors are likely to target R&E for financial purposes, attempting to extort victims for the release of sensitive data. Actors may be motivated to destroy police records or evidence to punish victims for nonpayment or to support criminal entities.

Attackers are most likely to gain initial footholds on a victim's network using a few specific methods. First, attackers are likely to exploit spearphishing links or attachments sent to police or dispatch officers. In addition, they're likely to exploit weak or unprotected remote desktop protocol ports. This is often achieved by brute forcing passwords, abusing known exploits or the exploitation of known vulnerabilities in public-facing applications.

LAND MOBILE RADIO

We assess that the Land Mobile Radio (LMR) communication systems used by first responders and federal agencies face a moderate threat to their confidentiality, integrity and availability. The most common attacks against public safety LMR in 2020 were the disruption of non-trunked radio traffic by hacktivists in response to the civil unrest in the United States.[12] Advanced Persistent Threat (APT) groups and insiders also target LMR communications.

ADVANCED PERSISTENT THREAT GROUPS

We assess with moderate confidence that APT groups will most likely target LMR systems with the goal of enabling or causing Denial of Service (DoS) conditions to accomplish political goals.

Political objectives for targeting LMR systems are assessed to include the disruption of federal law enforcement communications to hide or distract from APT or nation-state activity as well as to gain and maintain access to LMR systems in preparation for possible future political opportunities. This assessment is based on observed attack data aligning with APT TTPs and motivations.

These motivations, in addition to known APT methodology, align with observed attacks on LMR systems and adjacent networks. In one instance, a United States statewide law enforcement network was compromised in what is assessed by federal investigators to be a nation-state sponsored attack. The attackers were able to gain access to the agency's LMR system support network to deliver an undisclosed malware. Federal authorities ultimately determined that the greater LMR network was not exploited, though the access was used to help the actor target other victims. The support network compromise could have allowed the attackers to access the core LMR network or impact other adjacent systems used in public safety operations, such as law enforcement mobile digital terminals.

In a separate attack in 2018, LMR communications at a military base for an intergovernmental organization were repeatedly disrupted by an unknown adversary. A network switch at the base was disabled 15 minutes after the location's close of business. This caused a two-hour outage for radio communications. Two days later, the attacker disabled the same network switch and the local network, resulting in a second disabling of radio communications. The disruptions were purportedly possible due to implementation flaws in the base's underlying backhaul network. This allowed LMR communications to be disrupted via a single point of failure from the disabled network switch. Both outages at the base are assessed with high confidence to have been intentionally created and occurred during a period in which the base was shelled weekly by artillery.

Due to finite resources, many public safety organizations lack sufficient policies and controls needed to identify and prevent insider threats.

INSIDER THREATS

We assess with moderate confidence that an inside employee or LMR system maintainer will inadvertently or maliciously enable a DoS condition on an LMR system. When properly configured, LMR two-way radio systems are either completely isolated from the internet or have minimal internet-facing connectivity. Therefore, inadvertent configuration errors, insecure operational practices or a malicious insider are likely common factors of LMR system compromises. This is based on observed attack or system compromise data, reported misconfiguration errors and known insufficient cyber practices.

MALICIOUS INSIDER

A malicious insider with access to an LMR network can cause attacks which impact availability, integrity or confidentiality. In the past 5 to 10 years, police departments have been under increased scrutiny by many groups and hacktivist organizations, which may result in sympathetic insider activity. During a 2014 citywide protest in the United States, a sympathetic insider published sensitive information from the ad hoc radio network used by law enforcement to respond to the protest. The published information was used, likely in a coordinated effort, by low-sophistication hacktivists conducting repeated Distributed Denial of Service (DDoS) attacks to disrupt police communication, which was critical to the protest response operation.

Due to finite resources, many public safety organizations lack sufficient policies and controls needed to identify and prevent insider threats. This increases the likelihood that malicious activity goes undetected. Awareness campaigns can help stakeholders and employees learn to spot and report possible risky behavior causes, such as bankruptcy, divorce or involvement in dangerous ideologies. Establishing a baseline of accepted employee behavior can help identify suspicious activity including USB usage, irregular work hours or network (IP) address activity from unusual locations. Identifying workers potentially impacted by events such as reduction in force or pay can help prioritize monitoring efforts. Any monitoring efforts should conform with local and national laws regarding data storage and personnel monitoring.

INADVERTENT INSIDER

Insiders do not always operate with malicious intent. However, these inadvertent insiders can still pose a large risk to LMR systems. The most significant security lapses observed and reported were due to insufficient password rotation, poor patch management and malware-compromised USB sticks. In some cases, default or weak passwords were used for extended periods of time across entire LMR networks. The observed password behavior and poor cyber hygiene was purportedly due to a lack of established cybersecurity policies, inspection and adherence to accepted frameworks like the NIST CyberSecurity Framework, as well as a desire for ease of access.

Enabled by strained or understaffed software patch management programs at many public safety organizations, threat actors are also likely to exploit known vulnerabilities to gain system access. According to our internal research, approximately one-third of United States LMR systems do not have a robust software patch management strategy, greatly increasing their risk of compromise. More concerning, some LMR systems have been discovered to only have one update ever applied, negating the benefits of those subscribed to patching services. This is problematic since LMR systems are gaining greater connectivity through the CEN perimeter. In addition to the LMR operational components, CENs can contain numerous third-party applications, making it essential to ensure all components are patched on a regular and timely basis.

Another rare but impactful risk to LMR systems is USBs compromised by malware. Compromised USBs have been observed infecting and purportedly shutting down LMR systems with hidden viruses. In one instance, a USB drive was shared between a department's IT network and an LMR network, resulting in malware infecting the isolated LMR network. Some cyber threat actors, such as FIN7 and APT28, reportedly used malicious USB drops and USB backdoors in order to infect their victims. The fact that LMR systems typically contain minimal data that can be stolen may demotivate financially or espionage-motivated attackers. Still, they remain a possible target for attackers motivated by ideology or notoriety, such as hacktivists seeking to create DoS attacks for fame or in support of their cause.

TACTICS, TECHNIQUES AND PROCEDURES

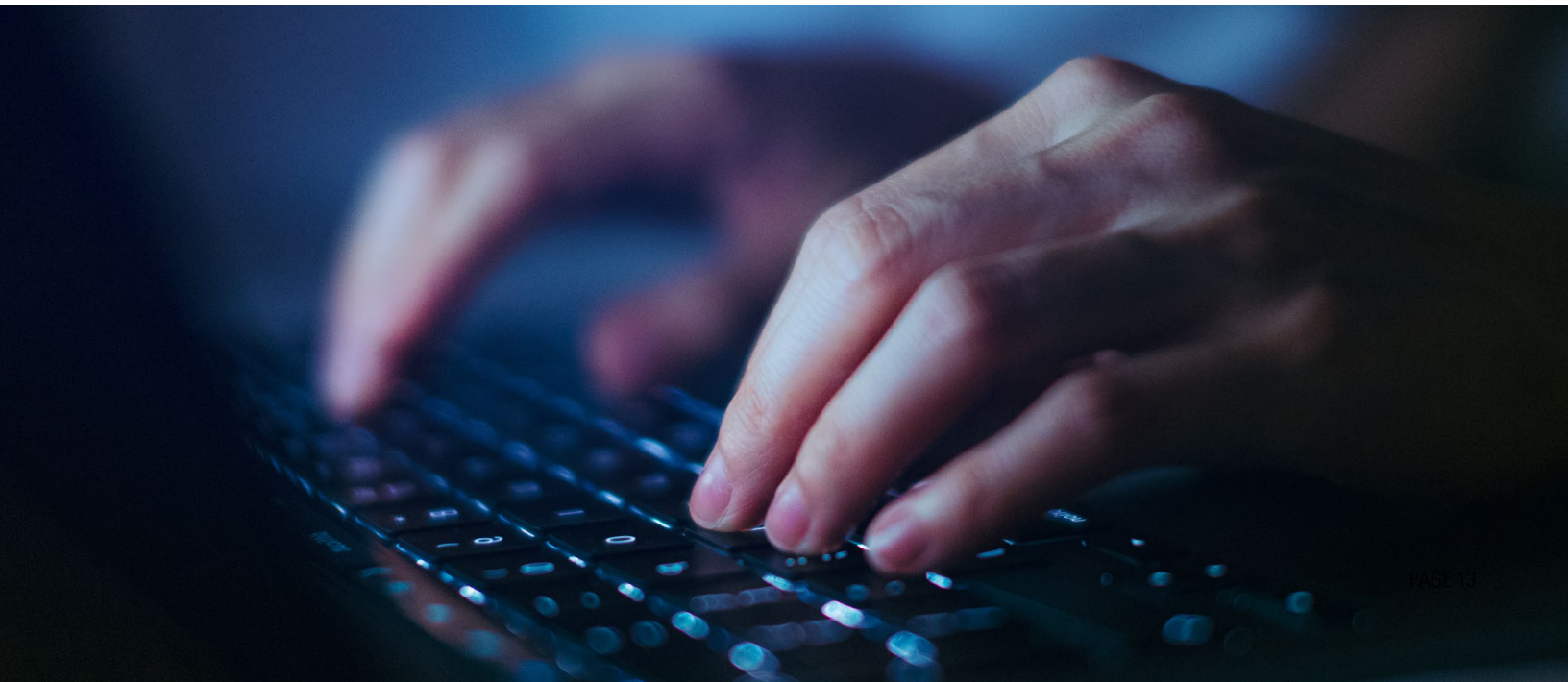
We assess with moderate confidence that attackers are most likely to use the TTPs below when targeting LMR (Figure 7). This is based on observed attacks against LMR systems and the historic targeting of critical systems by APT groups such as those affiliated with Russia.[13] Given the current observations, organizations should conduct threat hunting to confirm potential insider and APT activity aren't present in their environment.

Attackers, APTs or insiders are most likely to gain access to encrypted LMR systems via a few specific methods. These include: Hardware or Key Theft, such as stealing radios or voice over-the-air encryption keys; Inherent Access, such as from insiders who would already have access to networks or systems and Replication Through Removable Media. It is less likely, but still a real possibility, that attackers could use Valid Accounts to gain access to poorly-secured LMR systems. Audio Capture via live surveillance of radio broadcasts is the only observed TTP used by attackers to collect information, often to monitor the movements of law enforcement personnel. Attacks against LMR are most likely to result in Broadcast DoS attacks transmitted over radio channels to disrupt communication, Network Denial of Service and System Shutdown/Reboot.

Organizations should conduct threat hunting to confirm potential insider and APT activity aren't present in their environment.

INITIAL ACCESS	DATA COLLECTION	ATTACK IMPACT
Hardware or Key Theft	Audio Capture	Broadcast Denial of Service
Inherent Access (Insider Threat)		Network Denial of Service
Replication Through Removable Media		System Shutdown/Reboot
Hardware Addition		Data Encrypted for Impact
Valid Accounts		Service Stop
Trusted Relationship		Disk Structure Wipe

Figure 7: Heat map of TTPs observed against LMR, sorted in descending order of likelihood.



Public safety organizations face growing threats from criminals, nation-states, hacktivists and insiders across systems and platforms that were, until recently, self-contained and isolated.

SHARPENING THE PUBLIC SAFETY CYBERSECURITY TOOLSET

For public safety leaders and practitioners, today's threat environment can seem daunting. As the COVID-19 pandemic has reminded us, dependable, secure emergency services are essential for the normal functioning of society. Yet, that very truth is what makes public safety targets so enticing to threat actors.

Public safety organizations face growing threats from criminals, nation-states, hacktivists and insiders across systems and platforms that were, until recently, self-contained and isolated. The newly-connected nature of these technologies makes them more akin to IT systems, with all the inherent risk that comes with them. Therefore, it's essential to not only secure the tools themself, but also all traditional enterprise IT systems connected to them.

Public safety leaders must keep up by developing and implementing an in-depth risk management approach. To that end, agencies must first achieve a comprehensive understanding of how well security controls, policies and procedures are protecting enterprise networks, cloud environments and endpoints. In addition, they must ensure they have 24/7 monitoring, a comprehensive patch management system and good cyber hygiene in place for anything that may connect to public safety networks.

We believe that this report can inform that approach, sharpening the analytical toolset and empowering public safety organizations to better secure the critical systems citizens depend on.

GLOSSARY OF TERMS

TACTICS, TECHNIQUES AND PROCEDURES NOT ON THE MITRE ATT&CK FRAMEWORK:

- **9-1-1 Direct:** Threat actors may directly call emergency lines (such as 9-1-1 in the United States) to target local PSAPs in TDoS attacks.
- **Admin Line Discovery:** Threat actors may use the internet to research administrative lines belonging to PSAPs (such as 1-800 numbers) to conduct TDoS attacks.
- **Botnet Creation:** Threat actors may exploit victim devices via techniques like Drive-By Compromise to create botnets before conducting denial of service attacks. Created botnets are frequently used in TDoS attacks against PSAPs.
- **Botnet Purchase:** Threat actors may rent or purchase botnets via criminal marketplaces to amass the necessary machines to conduct denial of service attacks. This is often implemented in TDoS attacks against PSAPs.
- **Broadcast Denial of Service:** Threat actors may disrupt LMR communications for political, ideological or financial motivations by broadcasting false, confusing or arbitrary sounds and information across encrypted and unencrypted talk channels. This tactic is often used in conjunction with Hardware or Key Theft, especially in instances where encrypted channel communications are disrupted.
- **Call Spoofing:** When conducting TDoS attacks against PSAPs, threat actors may spoof the simulated phone numbers used in the attack. This can disrupt defender attempts to isolate and respond to fraudulent calls.
- **Critical Timing:** When conducting TDoS attacks against PSAPs, threat actors may position attacks during times in which defenders are unable to proactively respond due to high call volume or low staffing, like holidays or statewide events (such as the 2020 protests in the United States).
- **Data Extort/Publish:** Threat actors may steal data for the purpose of extorting victims for its release. In these instances, threat actors may publish portions of the data on custom, data-sharing sites. This behavior is often observed in association with extortion groups.
- **Execution Via Botnet:** Threat actors may use botnets to produce high amounts of traffic or simulated phone calls in TDoS attacks.
- **Hardware or Key Theft:** A common way for threat actors to gain access to LMR transmissions. Threat actors may use stolen radios or hardware encryption keys to surveil encrypted communications between first responders and federal officers. Threat actors may also use stolen radios or hardware encryption keys to conduct Broadcast Denial of Service attacks.
- **Inherent Access:** Malicious or inadvertent insiders are a common factor in compromises to LMR systems or transmissions. Inherent Access is the term used to describe attacks or events in which no outside action was necessary to gain access to LMR.
- **Telephony Denial of Service (TDoS):** A TDoS attack is an attempt to make a telephone system unavailable to the intended users by preventing incoming and/or outgoing calls. This is accomplished when threat actors successfully consume all available telephone resources, so that there is no unoccupied telephone line.

ADDITIONAL TERMS:

- **Administrative Lines:** Specific ingress phone numbers belonging to PSAPs (such as 1-800 numbers) that exist in addition to emergency lines used for 9-1-1 call routing.
- **Customer Enterprise Network (CEN):** The network containing the public safety organizations own computers and servers.

eCrime: The phenomenon of cyber targeting and attacks which are financially motivated and not directly tied to nation state-associated activity. Extortion groups like Maze, Conti, Sodinokibi and others often fall under this category as well as many of those who conduct low-sophisticated attacks like TDoS.

For more information about our Cybersecurity Services, contact your Motorola Solutions representative or visit **motorolasolutions.com/cybersecurity**

SOURCES

1 United States Cybersecurity and Infrastructure Security Agency. (n.d.). Alert (AA20-107A). Retrieved June 30, 2020, from https://us-cert.cisa.gov/ncas/alerts/aa20-107a
2 CROWDSTRIKE OVERWATCH TEAM. (2020, September 15). 2020 THREAT HUNTING REPORT INSIGHTS FROM THE CROWDSTRIKE OVERWATCH TEAM (Rep.). Retrieved September 15, 2020, from CrowdStrike, Inc. website.
3 CROWDSTRIKE OVERWATCH TEAM. (2020, September 15). 2020 THREAT HUNTING REPORT INSIGHTS FROM THE CROWDSTRIKE OVERWATCH TEAM (Rep.). Retrieved September 15, 2020, from CrowdStrike, Inc. website.
4 Abrams, L. (2020, June 09). Maze Ransomware adds Ragnar Locker to its extortion cartel. Retrieved June 10, 2020, from https://www.bleepingcomputer.com/news/security/maze-ransomware-adds-ragnar-locker-to-its-extortion-cartel/
5 Bing, C. (2016, November 14). DHS: Teenager's malware disrupted 911 call centers in 12 states. Retrieved July, 2020, from https://www.cyberscoop.com/911-call-center-ddos-dhs-maricopa-county/
6 SecureLogix Corporation. (2017). The Telephony Denial of Service (TDoS) Threat An Analysis of the TDoS Threat in Voice Network Security [PDF]. San Antonio: SecureLogix Corporation.
7 Claburn, T. (2019, July 02). Cop a load of this: 1TB of police body camera videos found lounging around public databases. Retrieved August 01, 2020, from https://www.theregister.com/2019/07/01/miami_police_bodycams_leaked/
8 Newman, L. (n.d.). Police Bodycams Can Be Hacked to Doctor Footage. Retrieved September 01, 2020, from https://www.wired.com/story/police-body-camera-vulnerabilities/
9 Stallman. (2020, March 30). Exploit. Retrieved March 30, 2020, from hXXps://exploitinqx4sjro[.]onion/topic/170111
10 Rose, J. (2020, June 08). Hackers Are Finding Footage on Police Body Cams They Bought on eBay. Retrieved June/July, 2020, from https://www.vice.com/en/article/8895ek/hackers-are-finding-footage-on-police-body-cams-they-bought-on-ebay
11 Bradbury, D. (2020, February 28). Ransomware wipes evidence, lets suspected drug dealers walk free. Retrieved February 29, 2020, from https://nakedsecurity.sophos.com/2020/02/28/ransomware-wipes-evidence-lets-suspected-drug-dealers-walk-free/
12 Bradley, B. (2020, June 02). Failure to communicate: CPD radio system exposed during protests, looting. Retrieved June 02, 2020, from https://wgntv.com/news/wgn-investigates/failure-to-communicate-cpd-radio-system-exposed-during-protests-looting/
13 Greenberg, A. (2017, June 20). How an Entire Nation Became Russia's Test Lab for Cyberwar. Retrieved August 15, 2020, from https://www.wired.com/story/russian-hackers-attack-ukraine/

MOTOROLA SOLUTIONS

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