2021 CYBER THREATS TO PUBLIC SAFETY

TECHNOLOGY FOCUS

Insights from the Motorola Solutions Threat Intelligence Team

MOTOROLA SOLUTIONS

MOTOROLA
POLICE
S.W.A.T.
F. PAGE
SERGEANT
CITY OF DALLAS
POLICE
4389
WATCH GUARD

As the global public safety technology leader, Motorola Solutions builds highly innovative solutions for law enforcement, fire, EMS, 9-1-1, and other state and federal agencies. Our commitment to delivering the best products and services for the public sector, with a focus on cybersecurity, gives us direct insight into the cyber threats that uniquely challenge first responders around the world. Since 2018, the Motorola Solutions Threat Intelligence Team has annually compiled their research and analysis to directly share this insight with public safety organizations.

In 2021, as we enter the second year of the COVID-19 pandemic, public safety, like other sectors, became more interconnected, with formerly disparate systems and data ever-more integrated. In this year's annual report, we share our findings on how this interconnectedness creates new risks, exacerbates known issues and requires new levels of vigilance.

To compile this report, the Threat Intelligence Team used proprietary, anonymized data along with both publicly reported and closed source cyber intelligence from January 1 - September 15, 2021, in addition to comprehensive research into the public safety technology space to identify the most pressing and significant threats, threat actors and risks to emergency services.

Knowledge is power. We aim to empower leaders and practitioners with the information they need to minimize risk and stay a step ahead of the most significant cyber challenges across the public safety mission-critical ecosystem. In sharing our research, we believe this report can improve the security and awareness of the critical agencies and organizations tasked with keeping all of us safe.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Identifying threat actors and their associated tradecraft helps us to make more specific recommendations for security.

As the world endured the second year of the COVID-19 pandemic, we became more agile, adaptable and interconnected. Our tools did, too. These tools allowed us to be productive and efficient no matter where we were. For public safety, this meant reliable and efficient emergency response while fending off increased threats to availability, integrity and confidentiality. Everything from radios, communication platforms, dispatching suites and video surveillance systems became more fundamentally linked, providing increased intelligence and streamlined capabilities. However, the benefits of these next-generation tools do not come without risk.

In 2021, cybersecurity threats became more sophisticated, persistent and widespread. Ransom payments increased 82 percent globally, while the fallout from extortion attacks increased due to the added technique of data theft.[1] Our Threat Intelligence team focused on better understanding the threats frequently targeting public safety. Identifying threat actors and their associated tradecraft helps us to make more specific recommendations for security.

Public Safety Answering Points (PSAPs), critical for routing emergency calls, remained the most frequent public safety target, most commonly hit with low-impact Telephony Denial-of-Service (TDoS) attacks. As a result of ever-increasing interconnectivity with other systems and devices, Land Mobile Radio (LMR) saw a slight increase in the number of compromises and security incidents, including malware infections and ransomware attacks. Video surveillance tools, such as license plate readers and fixed security cameras, represent a likely target for relatively unsophisticated actors who may try to increase the size of existing botnets or make a political statement through data breaches.

THE PUBLIC SAFETY TOOLKIT

LAND MOBILE RADIO

Land Mobile Radio (LMR) allows push-to-talk two-way communication between radio transceivers and can be built in many different variations, including handheld, vehicle-mounted and fixed base. It is utilized in a variety of industries, including public safety mission critical communications and private communications for commercial industries, such as oil and gas. Since LMR enables secure and instant communication, it is often a primary communication method in these industries, particularly in environments where cellular service is not practical because it is limited or nonexistent.

APCO INTERNATIONAL PROJECT 25 (P25) SYSTEMS

Traditional or enclave P25 LMR systems are not wholly isolated from the internet and should not be regarded as inherently secure. While they most commonly exist behind two firewalls, we have moderate confidence that enclave systems' network topography and high-privileged accounts could allow a patient or persistent attacker access in rare instances. This assessment is based on available network schematics and known deployment configurations.

Misconfigurations and not fully leveraging available security features are the most common pitfalls in P25 LMR systems. The use of built-in administrator accounts rather than non-privileged accounts for normal use, and missing or misconfigured firewall policies to segment the LMR network from adjacent networks are the most frequently reported misconfigurations for P25 systems. However, in some instances P25 systems that were configured correctly were not leveraging all of the available security features native to their systems, such as intrusion prevention systems (IPS) on hosts, which allowed attackers to go undetected. We encourage all P25 users to work with their providers to ensure they understand and apply as many security capabilities as possible that are natively available.

Vulnerability exploitation in remote access solutions can feasibly allow access to, or control over, a P25 core environment. Since the beginning of the Covid-19 pandemic the global cybersecurity community has seen a concentrated effort by malicious actors to find and exploit vulnerabilities in remote access solutions, such as VPNs. While not unique to P25 systems, VPN solutions by Palo Alto, Fortinet and Pulse Secure all serve as examples that were reported by CISA in 2020 and 2021 as having vulnerabilities which were exploited by malicious actors. VPNs are not inherently insecure. However, when vulnerabilities become known, applying recommended mitigations should be prioritized and in all feasible cases multi-factor authentication should be used for their accounts.

TETRA SYSTEMS

When compared to P25, TETRA has separate security concerns. Based on observations, TETRA environments allow remote connections in rare instances.

A potential exists of TETRA administrators who run connections from outside their IT networks, through firewalls, into TETRA systems. These connections are frequently managed by third-party remote access solutions.

In both the TETRA and APCO P25 environment cases, vulnerabilities in that firewall or the remote access solutions could feasibly allow an attacker to abuse these remote connections.

Users should rely consistently on best practices, such as regular patching, regular audit of and rotation of access credentials, and disabling unused ports and services to help mitigate this issue.

CYBER ATTACK DEVELOPMENTS IN LAND MOBILE RADIO

We last conducted a comprehensive review of the LMR threat landscape in mid-2020. Since then, the most significant shift in attacks to LMR systems is a minimal increase in Broadcast-Denial-of-Service (BDoS) and a minimal increase in Data Encrypted for Impact to LMR systems. The BDoS attacks occurred in concert with broader societal unrest, specifically when local governments enacted curfews and citizen-led protests were ongoing, especially during the summer of 2020. It is highly likely that these BDoS attacks were conducted in direct response to widespread protests and were ideologically motivated. Ransomware attacks impacting LMR were almost certainly financially-motivated and appeared to be enabled by misconfigurations and default passwords. Both the observed BDoS and ransomware attacks placed denial-of-availability (DoA) as the most common attack impact, with four out of five incidents resulting in DoA. Therefore, it is assessed with moderate confidence that any successful financial or ideologically-motivated attacks to LMR are most likely to result in an impact on LMR systems' availability, whether via the disruption of over-the-air communications or by encrypting radio management servers.

We previously observed non-technically sophisticated criminals using Hardware or Key Theft as a way to obtain access to encrypted law enforcement communications and to create their own private channels. That trend has continued since mid-2020. On June 22, 2020, the Toronto Police Department announced that its investigators had uncovered a scheme to provide stolen police radios to city tow truck drivers, and 11 individuals were charged. The criminal operation placed encrypted police equipment in the hands of several drivers who worked for multiple Toronto towing organizations.

These drivers planned to use the radios to survey police communications, thereby gaining an advantage in finding and arriving at the scenes of vehicular accidents before competitors. This "early-warning system" was especially valuable to tow truck drivers during the height of the COVID-19 pandemic shutdown in Toronto as fewer drivers were on the road, which reduced the number of overall accidents. Investigators seized three radios, six tow trucks and one gun as part of the arrests. Toronto Police arrested at least one officer in connection with the radio thefts.[2] Based on the prevalence of the Hardware or Key Theft tactic in unsophisticated compromises, we assess with high confidence that this method will remain popular, especially among individuals or groups who seek to either evade or monitor law enforcement.

During incident response and investigations of attacks to LMR systems, the Motorola Solutions Threat Intelligence Team was able to identify the tradecraft that attackers most commonly used, which included IP block scanning to the target system as well as vulnerability scanning as part of their initial reconnaissance efforts. In instances like the Toronto example above, less sophisticated threat actors frequently relied on "inherent access," using insiders to provide stolen radios or encryption keys. Meanwhile, more sophisticated threat actors used traditional access methods such as compromising external remote services and exploiting public-facing applications to intrude on vulnerable and exposed LMR networks and adjacent systems. Once in target networks, attackers were observed obtaining default domain accounts for elevated privileges.

Attackers were identified removing indicators off hosts during an attack to evade detection and attribution. In all observed, researched or assessed instances of LMR compromise, attackers either conducted a BDoS attack or executed ransomware to encrypt data when not seeking to surveil law enforcement communications or establish their own, clandestine channel.

Vulnerabilities in that firewall or the remote access solutions could feasibly allow an attacker to abuse these remote connections. It is recommended that users rely consistently on best practices, such as regular patching and disabling unused ports and services, to help mitigate this issue.

LMR MITRE ATT&CK MAPPING

RECONNAISSANCE	INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	DEFENSE EVASION
█ Scanning IP Blocks	█ Hardware/Key Theft	▓ PowerShell	▓ External Remote Services	▓ Bypass User Account Control	█ Indicator Removal on Host
█ Vulnerability Scanning	█ Inherent Access (Insider Threat)	▓ Windows Command Shell	░ Create or Modify Windows Process	▓ Process Injection	▓ Disable or Modify Tools
	█ Replication Through Removable Media	▓ Unix Shell		▓ Exploitation for Privilege Escalation	▓ Disable Windows Event Logging
	▓ External Remote Services	▓ Windows Management Instrumentation (WMI)			▒ Obfuscated Files or Information
	▓ Exploit Public-Facing Application	▓ Service Execution			▒ Match Legitimate Name or Location
	▓ Default Accounts	▒ Native API			▒ Modify Registry
	▓ Domain Accounts	░ Python			░ Signed Msiexec Execution
	░ Compromise Software Dependencies and Development Tools				░ Signed Regsvr32 Execution
	░ Compromise Software Supply Chain				░ Signed Rundll32 Execution

CREDENTIAL ACCESS	DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND & CONTROL	EXFILTRATION	IMPACT
▓ Password Spraying	▓ Process Discovery	▓ Lateral Tool Transfer	█ Audio Capture	▓ Encrypted Channel	░ Exfiltration Over C2 Channel	█ Broadcast-denial-of-service (BDoS)
▓ Credential Stuffing	▓ Network Service Scanning	▓ Replication Through Removable Media	▓ Data From Local System	░ External Proxy	░ Exfiltration Over Symmetric Encrypted Non-C2 Protocol	█ Data Encrypted for Impact
▓ Password Guessing	▓ System Information Discovery	░ Remote Services (if applicable)	░ Data From Configuration Repository	░ Non-Standard Port	░ Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	▓ System Shutdown/ Reboot
▒ OS Credential System Dumping	▓ System Service Discovery				░ Exfiltration Over Unencrypted/Unobfuscated Non-C2 Protocol	▓ Data Destruction
▒ Credentials in Files	▒ Domain Groups Discovery					▒ Resource Hijacking
	▒ System Network Connections Discovery					▒ Service Stop
	▒ Network Share Discovery					▒ Inhibit System Recovery
	░ File and Directory Discovery					░ Network-denial-of-service
	░ Network Sniffing					

LEGEND
█ Likely
▓ Probable
▒ Possible
░ Unlikely / Rare

RECOMMENDED ACTIONS

The increasingly connected nature of LMR systems doesn't pair well with the rise in sophisticated attackers. This combination requires LMR operators and technicians to ensure a layered, enforced and comprehensive security approach. It also requires LMR users to ensure those native security controls are implemented at time of installation, during operation, and complemented with administrative controls, policies and procedures.

Multi-factor authentication must be enabled and enforced for all available accounts accessing the DMZ and core of an LMR system. Compromised access devices can introduce a variety of threats to LMR cloud environments as defined by The National Institute of Standards and Technology in their mobile threat catalog.[3]

Finally, procedures for reporting lost or stolen equipment, regular inventory auditing of radio equipment, as well as for disabling that equipment should be implemented wherever possible. This can help to identify when the Hardware or Key Theft TTP is usable by insiders and low-sophistication actors.

PUBLIC SAFETY ANSWERING POINT SUITE

THE PUBLIC SAFETY ANSWERING POINT

Public Safety Answering Points (PSAPs) are centers that process emergency calls. They typically have five primary communication flows: inbound 9-1-1 calls, inbound SMS traffic, outbound locational queries, outbound dispatch traffic and bidirectional administrative lines. This critical infrastructure enables emergency responders to be informed of and respond to significant events affecting the public. With the implementation of IP-based telephone networking services and evolving technology, PSAPs must be prepared to actively manage possible cybersecurity threats, including telephony denial of service attacks (TDos), ransomware and other unauthorized access to data and systems. With the increased use of IP-based platforms and the accompanying increase in attack surface, the risk of cybersecurity attacks and other threats against PSAPs will likely increase.

CALL HANDLING

Call Handling is accomplished through IP and telephony-based software used to accept, queue and answer emergency calls. Current generation call handling systems can also accept SMS-based messaging. In the future, it is expected that these solutions will process other forms of emergency messaging traffic, such as multimedia.

One of the most significant threats to PSAPs is TDoS attacks via physical and IP-based telephony lines.[4] Threat actors leverage TDoS attacks against 9-1-1 and administrative phone lines, both of which can result in disruptions to call handling ability. While these attacks often go unreported, they remain the most common attack type we have observed involving PSAPs. These attacks are extremely easy to conduct, requiring little to no sophistication.

An attacker can conduct a TDoS in two ways: manual and automated. For manual TDoS attacks, threat actors must access an arbitrary, but often high, number of phones. These are either prepaid disposable phones or phones compromised with malware. In either scenario the attacker can leverage these devices by having them dial emergency numbers, flooding PSAPs with manually-generated calls.

Automated attacks are easier to conduct. They only require access to a virtual telephony system capable of fielding a large number of computer-generated calls. This can be accomplished by renting access to low-cost botnets or even by running simple programs via desktops or other workstations.

The motivations behind TDoS attacks range from ideological to financial or even notoriety. However, available reporting from victims suggests it is likely that low-sophistication attackers primarily seek to make money in TDoS schemes by extorting PSAPs for a ransom. These financially-motivated TDoS attackers are often unaffiliated with specific groups, instead choosing to act alone.

Next Generation 9-1-1 (NG9-1-1) systems are more resilient to TDoS attacks than legacy systems since they are capable of handling a much higher number of simultaneous calls than older systems. However, TDoS attacks are still a problem for NG9-1-1. While NG9-1-1 systems are able to withstand the flood of calls fielded by TDoS attackers, PSAP employees on the receiving end of these calls are not so lucky.

In older, non-NG9-1-1 systems, TDoS attacks impacted service provider phone lines due to call loads being higher than telephony bandwidth. In NG9-1-1, those fraudulent calls are going through, resulting in call-takers having to answer them. “Real” calls intermingle with these fake ones, as everyday citizens attempt to contact emergency services. This results in people having to wait longer for their calls to be answered, which often lead to abandoned calls and redials, effectively creating another TDoS within the original attack.

When conducting TDOS attacks against PSAPs, threat actors may position calls during times in which defenders are unable to proactively respond due to high call volume or low staffing. Statewide protests or natural disasters like wildfires can result in a high number of legitimate 9-1-1 calls. Meanwhile, off-hours and some holidays can mean fewer dispatch personnel at work. Either of these situations will worsen the disruptive effects of TDoS attacks.

COMPUTER-AIDED DISPATCH (CAD)

Dispatchers, call handlers and 9-1-1 operators leverage Computer Aided Dispatch (CAD) systems to send emergency personnel to where they’re needed most. Dispatchers also use CAD systems to identify first responder location and status, in addition to prioritizing and recording incoming emergency calls.

Ransomware is the most common threat to CAD, impacting CAD systems in two ways. The first is via indirect attacks on municipal and police networks. These municipal and police environments often work as the backbone networks for CAD systems. In the event of a ransomware attack, defenders may disable network services as a precaution, as part of incident response, or during later data restoration activities. Each of these scenarios can result in disruptions to CAD services.

The second way in which ransomware can impact CAD systems is during a direct compromise of CAD networks themselves. Direct compromise is rarer, but does occur — especially when exacerbated by misconfigurations or unsecured services. Direct compromises of CAD networks often come from trusted connections between the CAD environment and adjacent municipal or police networks. They also occur when CAD workstations are enabled with outbound internet connectivity, a practice that is not the standard and is not recommended. Finally, inbound services such as VPN connections can be compromised in rare instances, leading threat actors to access CAD systems from the open internet or other networks.

RECENT DEVELOPMENTS

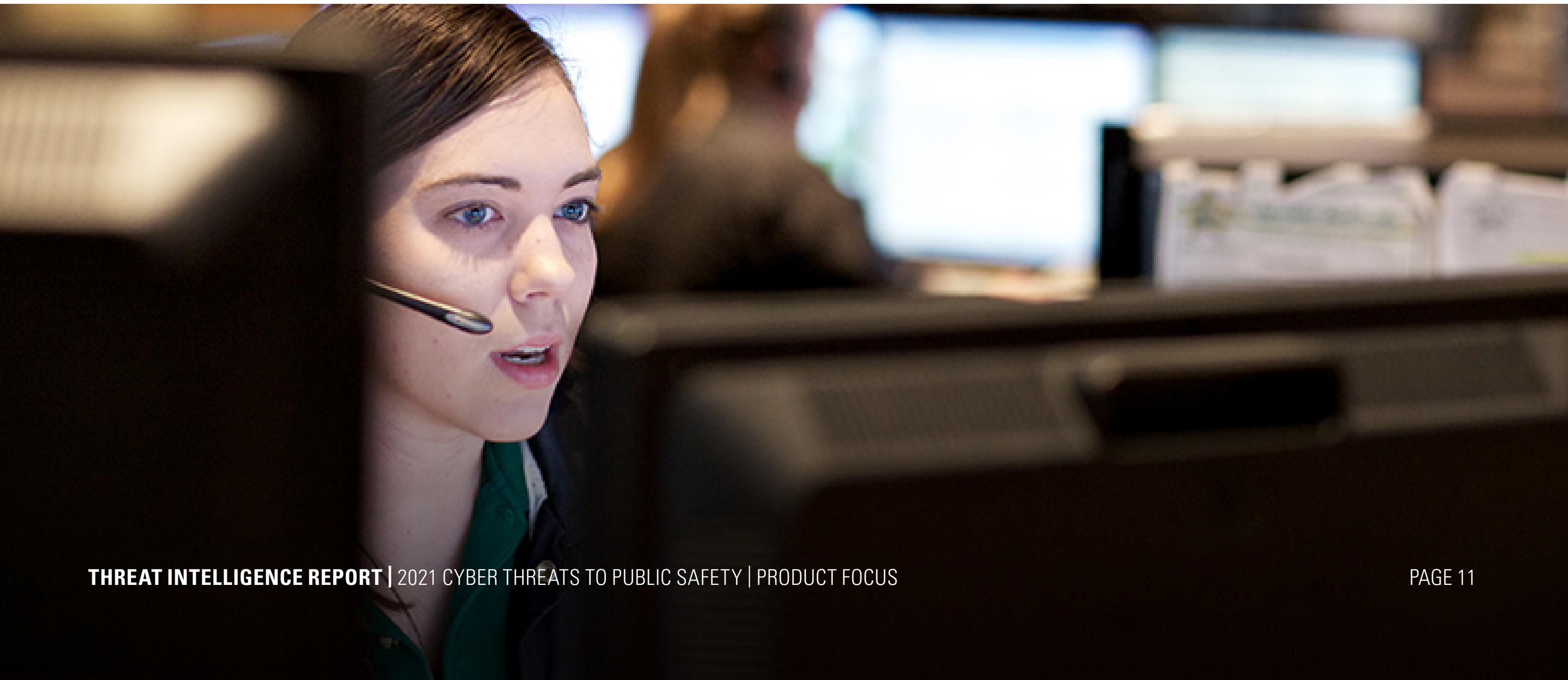
ATTACK SHIFTS

We last conducted a comprehensive review of the PSAP threat landscape in August 2020. Since then, attacks on PSAPs have increased. There was a 38 percent jump in reported attacks over the second half of 2020 and the beginning of 2021. This was largely due to five TDoS attacks against dispatch centers in the United States, resulting in the degradation of call-taking and handling services in each instance. In the previous reporting period, there were zero reported TDoS attacks. However, these events are rarely disclosed and, therefore, it can be stated with high confidence that TDoS attacks likely occurred but were not recorded. A state threat assessment notification published in May 2021 noted a "widespread increase in telephony denial of service attacks" to nationwide PSAPs. Based on this analysis, the observed increase in TDoS attacks since August 1, 2020, could indicate that there are either more of these events occurring, or that reporting has increased. We cannot reliably determine which is true at this time.

There was a 42 percent decrease in ransomware attacks impacting PSAPs, with only four reported since August 1, 2020. The decrease in observed ransomware attacks to PSAPs does not have a sole cause. However, it can be partially attributed to United States municipalities' increased preparedness against ransomware attacks. Additionally, communications from organizations like the Cybersecurity and Infrastructure Security Agency pushed the implementation of best practices such as offline data backups. This likely led to fewer instances of municipal networks and dedicated backups being encrypted. As such, impacts to connected PSAP networks are assessed to have decreased because of fewer instances where backbone municipal networks went down or were disabled during the towns' incident response efforts.

There was only one incident in which the malware behind a ransomware attack was identified with any confidence. On June 24, 2021, an unidentified threat actor(s) successfully compromised a dispatch center in the southern United States. Defenders responded by disabling two virtual machines and a virtual private network (VPN) service which the attacker(s) had accessed. A '.eight' file extension appended files infected during the attack. We believe the actor(s) used a variant of the Phobos ransomware and therefore may have been an affiliate or customer of that ransomware operation.[5] This assessment is based on the fact that the '.eight' appellation's ransom note shares similarities to Phobos ransomware notes and is used as a file extension by Phobos. The '.eight' malware variant is most often distributed via phishing emails with malicious attachments, unsecure torrent websites and malicious websites.

Physical attacks that did not rely on cyber capabilities remained unchanged over this reporting period, with one identified in the previous period and one occurring on December 25, 2020. The latter consisted of domestic terrorist Anthony Quinn Warner detonating an explosive in his van next to an AT&T network hub in Tennessee, killing himself and injuring three others. The blast caused a widespread communication disruption across the state. Cellular, wireline telephone and internet services were affected, as were multiple local 9-1-1 and non-emergency phone networks in the region. It is probable that any physical attacks against PSAPs are unlikely to be motivated by financial gain and are instead more likely to be motivated by personal, group ideological or terrorist intentions.

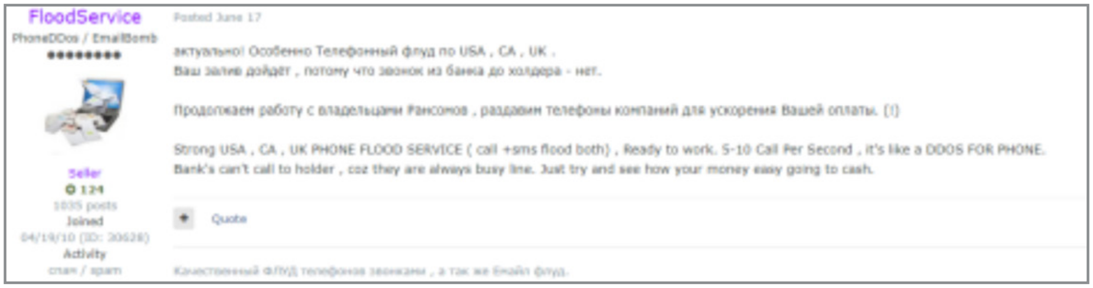


CRIMINAL FORUM ACTIVITY

The Motorola Solutions Threat Intelligence Team observed individuals offering services that could conceivably be used in TDoS attacks (See Figure 10). As mentioned above, TDoS attacks are conducted virtually. This is an evolution from the default method of using a host of infected phones to call 9-1-1, which was the case in the 2016 manual TDoS attack orchestrated by an Arizona teenager.[6] The reliance on virtual TDoS attacks developed due to the prevalence of voice-over-IP (VoIP) technology, which allows individuals to send an arbitrary number of "phone calls" without first having to obtain access to a wide array of phones. We previously assessed that it was likely these virtual TDoS attacks were sourced from botnet activity, specifically machines with VoIP capabilities sold on the dark web or criminal forums.

The reliance on virtual TDoS attacks developed due to the prevalence of voice-over-IP (VoIP) technology, which allows individuals to send an arbitrary number of "phone calls" without first having to obtain access to a wide array of phones.

There were multiple members observed selling "telephone flooding" services on underground forums, with prices as low as $3 USD per hour. These flooding services included virtual phone calls and SMS flooding capabilities, with one user describing it as a distributed-denial-of-service (DDoS) attack for phones. While there were zero instances of public safety targets or technologies mentioned in association with these flooding services, we believe with high confidence that these resources could be used against PSAPs — specifically against call taking and handling systems. It is likely that call flooding services such as these are used by many of the individuals or groups behind TDoS attacks.


FloodService
PhoneDDos / EmailBomb
●●●●●●●●●
Seller
124
1035 posts
Joined
04/19/10 (ID: 20628)
Activity
спам / spam

Posted June 17

актуально! Особенно Телефонный флуд по USA , CA , UK .
Ваш залив дойдет , потому что звонок из банка до холдера - нет.

Продолжаем работу с владельцами Рансомов , раздавим телефоны компаний для ускорения Вашей оплаты. (!)

Strong USA , CA , UK PHONE FLOOD SERVICE (call +sms flood both) , Ready to work. 5-10 Call Per Second , it's like a DDOS FOR PHONE.
Bank's can't call to holder , coz they are always busy line. Just try and see how your money easy going to cash.

Качественный флуд телефонов звонками , а так же Емайл флуд.

FIGURE 10: Underground forum user 'FloodService' selling call and SMS flooding.

RECOMMENDED DEFENSES

The interconnected nature of PSAPs, both with call-taking/handling services and CAD networks, require product designers to implement a layered, enforced and comprehensive security approach. Inbound VPNs; connections to adjacent, municipal networks; broadly-used domain accounts; and occasionally internet-enabled workstations are all potential security risks that could facilitate an attack against CAD systems within PSAPs. Meanwhile, TDoS attacks cannot be reliably defended against. Creating backup options for when 9-1-1 or emergency calling is disrupted can help to give citizens the chance to still interact with call handlers during emergencies. Posting non-emergency phone lines on social media sites has thus far been the most common tactic used by defenders while in the midst of TDoS attacks. However, those phone lines can also be targeted by TDoS attackers, so rerouting calls to nearby counties is a common practice.

Implementing MFA, where applicable and appropriate, can serve to limit the danger of compromised VPN credentials. Recent executive orders in the United States pushed the modernization and implementation of stronger cybersecurity standards through zero-trust architecture. Those orders included a mandate for MFA to ensure federal systems are protected from growing ransomware threats.

Any allowances toward internet-connected workstations within PSAP networks should be documented, as internet-connected workstations pose a risk and are a likely vector for ransomware infections.

Finally, as mentioned above, one of the most common disruptions to PSAPs happens when an adjacent or "backbone" municipal network is disabled as a result of a ransomware infection. In these instances, even when the PSAP network itself is not directly compromised, degradation of services or even outages may occur. As such, dispatch centers should expect that extortion attacks on municipal networks have a significant chance to also impact CAD or 9-1-1 call-taking/handling functions.

VIDEO SURVEILLANCE

FIXED VIDEO

CURRENT STATE OF CAMERAS AND NEW SECURITY RISKS

The development of fixed video technology allows sophisticated monitoring and alerting of irregular or malicious activity in physical environments. To accomplish next-gen video surveillance, fixed video solutions migrated from analog to IP-based cameras. This creates a new and significant threat vector that increases the threat surface for previously isolated systems.

Many customers of fixed video solutions may not fully understand the increased threats as a result of this transition. This has resulted in a large number of fixed surveillance systems going unpatched, unmonitored and unsecured.

Of the one million exposed cameras and 125,000 exposed servers identified by Shodan, 90 percent were exposed over HTTP, 8 percent over telnet, 8 percent over SSH and 3 percent over MySQL. These types of exposures could allow remote attackers to gain access to surveillance networks, facilitating criminal operations due to known, unpatched or yet-to-be-discovered vulnerabilities in the protocols or in the products themselves.[7]

Further, new IP-based camera systems are being integrated into cloud offerings, allowing remote access, viewing and control of camera networks. The additional cloud access increases the opportunity for misconfiguration or exposed accounts and keys which could allow threat actors to gain access to entire customer sets, or individual camera networks. For example, on March 9, 2021, hacker collective "APT69420," also referred to in public sources as "Arson Cats," discovered hardcoded credentials for a Verkada super administrator account in internet-exposed DevOps infrastructure.

Any and all DevOps environments exposed to the internet could result in a critical security failure that threat actors heavily target in their reconnaissance, as more often than not, sensitive credentials and access keys are hardcoded or exposed as a result of insecure practices. Proper and frequent audits and enforced security policies are essential for development teams to inhibit any unintentional exposure. In the Verkada incident, the hard-coded "super administrator" accounts in the exposed DevOps environment allowed the threat actors to view all customer surveillance footage that was supported by the cloud service.[8]

THREAT LANDSCAPE

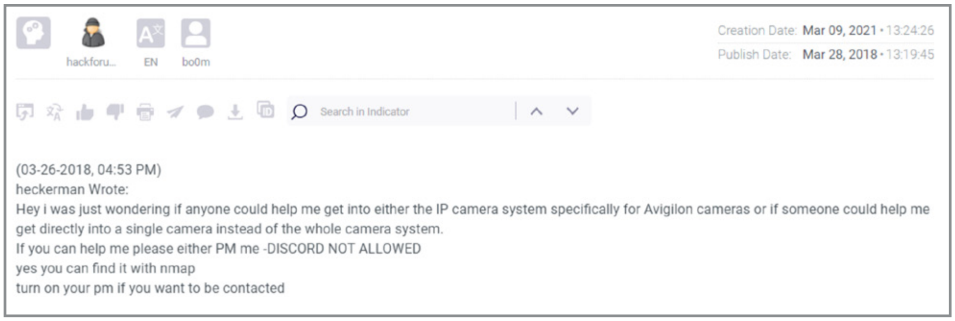
We have moderate confidence that the threat actors most likely to target fixed video surveillance are not very sophisticated. This includes ideologically-motivated hacktivists, financially-motivated botnet or crypto-mining operators and notoriety-motivated script-kiddies.[9] We base this assessment on the TTPs used by actors in observed compromises as well as the low prevalence of valuable data in fixed video systems when compared to other public safety technology.

It is unlikely, but possible, that IP camera networks may also be targeted by more sophisticated threat actors to facilitate criminal or espionage activity on adjacent enterprise networks, but would likely require misconfigured system deployments connected to adjacent enterprise networks or the open internet. Fixed video surveillance systems are assessed with moderate confidence to represent minimal financial value to sophisticated threat actors.

Fixed video systems are often deployed in schools, stadiums, manufacturing locations and governmental sites. The data stored by these systems is rarely vital to those organizations' day-to-day functions. Therefore, fixed video is unlikely to be purposefully targeted by accomplished eCrime groups. Likewise, fixed video data rarely contains valuable intelligence and does not represent a likely target for espionage campaigns. As such, no prominent or known to be sophisticated threat groups have been observed or identified targeting fixed video systems. However, since maintaining and protecting the privacy of those being monitored, such as in the case of schools, protecting video security assets is essential to ensure video feeds cannot be exposed.

The most frequent threat against fixed video surveillance systems is absorption into botnets, resulting in possible degradation of service. On October 12, 2016, the Mirai botnet scanned the open internet for Telnet ports.[10] The botnet then leveraged a combination of 61 username/password combinations frequently used as default credentials in internet-of-things (IoT) devices to attempt to log in to identified systems. Included in these IoT systems were fixed video IP cameras. After infecting the IP cameras and other IoT devices, the Mirai botnet launched a large-scale distributed-denial-of-service (DDoS) attack against the DNS infrastructure organization Dyn, disrupting internet services for the east coast of the United States. At the botnet's peak, there were roughly 600,000 simultaneous instances of IoT devices infected.[11]

Since 2016, the IRCTelnet botnet compromised IP cameras over Telnet via brute-force attempts and default credentials in a similar fashion to Mirai, though to a lesser extent.[12] Botnets target IoT devices for inclusion in DDoS attacks like Mirai, but also for cryptocurrency mining. Other individuals have displayed interest in gaining access to fixed video and Avigilon systems, (see Figure A below). This is most likely to facilitate follow-on behavior such as creating or enlarging a botnet and exposing video data, but may also allow extortion activity in rare instances. The above behavior is represented by the following TTPs: Remote Services, Default Accounts, Password Guessing, Resource Hijacking and Network Denial of Service.[13]



Creation Date: Mar 09, 2021 • 13:24:26
Publish Date: Mar 28, 2018 • 13:19:45

(03-26-2018, 04:53 PM)
heckerman Wrote:
Hey i was just wondering if anyone could help me get into either the IP camera system specifically for Avigilon cameras or if someone could help me get directly into a single camera instead of the whole camera system.
If you can help me please either PM me -DISCORD NOT ALLOWED
yes you can find it with nmap
turn on your pm if you want to be contacted

FIGURE A: Hackforums user 'heckerman' asking about gaining access to Avigilon IP camera system.

On March 9, 2021, threat actors reportedly gained access to managed surveillance camera company Verkada and had access to 150,000 live cameras installed across their entire customer base. The threat actors purportedly gained access to surveillance systems by using a discovered super admin account for Verkada in DevOps infrastructure that was exposed to the internet. From there, the threat actors were able to capture screenshots and access live video feeds and archived video. It is assessed with moderate confidence that the attackers only had access to camera feeds being managed by Verkada's cloud offering. This is based on some of Verkada's customers confirming that none of their on-premise video storage systems were compromised in the attack and that only cameras connected to Verkada's cloud services were exposed. Other impacted Verkada customers include Madison County jail in Huntsville, Alabama; Arizona's Graham County detention center; and an unnamed police station in Stoughton, Massachusetts. The TTPs identified in the hack included: Valid Accounts, Video Capture and Audio Capture.

Fixed video surveillance systems may be targeted as part of further access operations. On January 17, 2017, two low-sophistication Romanian individuals compromised Washington, D.C.'s Metropolitan Police Department cameras in an unsuccessful ransomware scheme.[14] This resulted in a four-day loss of availability to the cameras as they were taken offline during remediation efforts. The actors targeted the surveillance cameras with the intention of using them as a foothold into adjacent networks and used RDP to move laterally from compromised cameras into 123 connected computers.

The threat actors made several mistakes, including choosing to send ransomware via 179,000 individual emails using a bulk email service rather than compromising a domain controller and executing ransomware from that elevated position.[15] The actors also displayed poor operational security by using a Gmail account with one of the operator's names as a recovery address for a separate account that was linked to the attack, demonstrating their lack of sophistication. The initial method of access in the Washington, D.C. compromise is not reported. While the attempt was unsuccessful, it serves as an example of how IP camera networks may be only the initial target of attackers in uncommon instances.

CURRENT AND RECOMMENDED DEFENSES

Attackers most likely to target fixed video solutions are likely of low sophistication. Therefore, ensuring foundational security controls are enforced at the product level, as well as ensuring that third-party vendors are using best practices when working with their customers can help inhibit and deter most attacks.

Well-secured fixed surveillance cameras should be shipped without default passwords. They should also have signed, encrypted firmware. Ideally, each camera family should have a unique, derived encryption key that can be revoked at will. Additionally, cameras should be shipped with onboard encryption cards to mitigate the impacts of theft and tampering. The end users, however, must ensure they are patching and updating their cameras from a designated source offered by their provider to ensure they aren't exposed to any known vulnerabilities and exploits, which could bypass security controls.

In the end, consistent and thorough security falls upon end users. For instance, even when a product itself is secured, if there is no password length or complexity requirement to access it, the barrier for access is significantly reduced due to the risk of exposed or leaked credentials. The misconception around the connectivity of IP cameras to the internet has resulted in a significant number of end users failing to patch their cameras, as they commonly do not classify the cameras as part of their OT systems. While many cameras are secure on their own, they require effective management and installation in addition to sustained and comprehensive monitoring solutions.

Based on events like the Verkada hack, it is critical that IP camera systems, cloud environments and development environments are isolated from the open internet. There is no known legitimate reason for an IP camera network to allow Telnet or HTTP traffic to unprotected, unmonitored and unauthorized systems. Third-party sellers should be vetted for demonstrated security best practices. This will help ensure that those helping camera customers install and configure surveillance camera products are both capable of, and willing to, use secure best practices to protect their customer's mission.

Historical video service attacks have highlighted the importance of access control. Vendor access should be limited to only when the customer allows it and only for individual sessions. Further, it is recommended that audits and penetration tests are regularly conducted and that granted access is carefully monitored to ensure this remains the case.

In addition to separating IP camera networks and cloud environments from open internet systems, they should also be isolated from adjacent enterprise networks, including DevOps environments. At the time of deployment, limiting access to and from video networks is a best practice that should be shared via product documentation with prospective third-party sellers. This can help to mitigate potential large-scale compromises in the event that IP camera networks are used to gain opportunistic access to larger organizational or consumer networks.

LICENSE PLATE READERS (LPR)

PREVIOUS TARGETING AND COMPROMISE OF LPR SYSTEMS AND DATA

We identified four incidents impacting the license plate reader (LPR) space since 2015, in addition to the identification of vulnerable and exposed LPR systems through Shodan scans. The majority of these cases involved devices, databases and/or web portals that were openly accessible over the internet, without requiring authentication. One of the four incidents occurred as recently as April, 2020.[16] Our team only uncovered one case of a threat actor compromising an LPR business: a ransomware attack against Perceptics in May 2019. The extortion group Team Snatch compromised Perceptics in what was one of the earliest examples of extortion groups using both ransomware and data theft as a tactic and exfiltrated 449 gigabytes of data from the company. This included files owned by one of Perceptic's customers, the U.S. Customs and Border Protection agency. Stolen data included photos of faces and licenses of over 100,000 travelers driving in and out of the United States. We are not aware of which method(s) the attacker used to gain access to Perceptics' network. There is no indication that the breach was due to a vulnerability in the LPR technology stack itself or that the attack was motivated by the company's involvement in the LPR business. After Perceptics failed to pay the ransom demand, Team Snatch provided the stolen files to the moderators of the hacktivist leak site, DDoSecrets. DDoSecrets moderators then published the Perceptics data in June, 2019. The attack resulted in CBP banning further use of Perceptics within the organization and by federal contractors.[17]

CYBER CRIMINALS

Selling stolen financial personally identifiable information from compromised networks, individual infected computers, leaked databases or phishing attacks remains one of the highest priorities of cyber criminals.

Over the past year, our team found minimal discussions within the criminal underground regarding LPR technology, companies or other LPR products. Our investigation into dark web and open sources did not identify any dedicated criminal forum or group focused on LPR intrusions or the misuse of plate data derived from LPR recorded data. We did not find discussions of planned direct attacks on companies whose primary business operations revolve around the creation or maintenance of LPR technology on dark web forums.

Instead, we identified a trend of underground actors willing to share links to open-source reporting or resources to assist in identifying vulnerable LPR devices or IoT devices, particularly on code repositories such as GitHub.[18]

A majority of references to companies that provide LPR products did appear within prominent underground marketplaces such as Genesis Store, Russian Market or Amigos Market, but were likely affiliated with the compromise of consumer accounts, rather than administrative accounts. Further, underground forums and messaging services are being used widely by participants interested in more technical components within IoT technology, specifically CCTV camera systems, rather than LPR products or data, indicating a lack of financial value available in LPR technologies and data for cyber criminals.

We did not identify specific references to criminal misuse of LPR technology. Rather, the intelligence being shared and discussed could be used by a threat actor to gain knowledge on technical components as well as learn best practices from other participants.

Discussions of planned direct attacks on companies whose primary business operations revolve around the creation or maintenance of LPR technology were not discovered on dark web forums.

HACKTIVISTS

LPR remains a controversial technology, with critics claiming they represent increasingly pervasive surveillance and intrusion into privacy.[19] We judge this may motivate hacktivist threat actors to target LPR systems, with the aim of generating publicity and exposing insecure systems. It is likely that LPR providers and users will represent a target for politically-motivated hacktivist threat actors for reasons similar to the Verkada breach: striking against the perceived overreliance on public surveillance. We have not, however, obtained any specific intelligence on current intent to attack LPR systems.

We examined open-source forums, messaging services and security-related websites for content related to LPR technology as well as LPR suppliers or products. In our investigation, we did identify a number of forums, for specific brands, where users discussed the aforementioned topics, but we did not identify content we deem malicious that related to LPR exploitation or the targeting of any aforementioned systems. Analysis of a sample of forum threads identified the following themes:

- They did not identify users discussing vulnerabilities within LPR components, specifically in software that could be used for malicious purposes.
- Conversations about LPR, both on the basics of the technology and how it purportedly exacerbates the perceived problem of over-surveillance.

Our team observed a decrease in international hacktivist activity overall, as the hacktivist landscape shifted away from broad public participation and back toward its origins as a practice of smaller groups of dedicated individuals. As such, hacktivism-related attacks usually resulted in one of the following effects:

- Denial-of-service
- Defacement of public facing websites and portals
- Public exposure of sensitive data

NATION-STATES

We did not uncover any specific cases of state-sponsored threat actors seeking to covertly access LPR systems or LPR-generated data. We judge that at least some state-sponsored groups would have an interest in obtaining such data for intelligence purposes, for example, to track the movements of overseas individuals of interest. Yet overall, we assess that this would likely not be considered a top-priority data set to obtain.

COMMON VULNERABILITIES AND INFECTION METHODS

License plate reader cameras fall under the umbrella of IoT devices. These devices are commonly targeted and compromised for the purpose of creating a botnet, often via the overuse of default credentials or threat actors brute-forcing weak passwords. These botnets are often used to carry out DDoS attacks. However, the majority of observed compromises to LPR systems themselves were simply the result of exposed service provider networks lacking authentication.

One theme our team identified within the criminal underground was an interest among actors to share research or techniques to identify vulnerable IoT technologies capable of being exploited. However, mentions of LPR technology in association with these queries were still minimal.

We discovered one instance of discovered vulnerabilities pertaining specifically to LPR cameras. On January 21, 2021, a researcher from Macedonian firm Zero Science Lab published details of nine vulnerabilities affecting several models of LPR cameras sold by Selea, an Italian designer and manufacturer. Selea appears to be a relatively small company without a large market share. The vulnerabilities were subsequently published on a number of vulnerability and exploit repository sites, such as exploit-db.

The nine vulnerabilities included an unauthenticated directory traversal vulnerability which would allow an attacker to retrieve credentials and a post-authentication remote command injection vulnerability.

These two vulnerabilities could be easily chained together to allow unauthenticated remote code execution. There was only one mention of these vulnerabilities found on the dark web or underground forums and there is no further context around this reference to indicate whether there was any significant interest. We did not uncover any indications that these vulnerabilities had been or are being actively exploited.

LPR INDUSTRY FUTURE OUTLOOK

It is likely we will see further instances of inadequately protected LPR data, including devices or access portals being openly accessible over the internet.

As with Perceptics, LPR companies may become targets of ransomware campaigns, although we do not believe that it would specifically be their involvement in LPR technology that enables or motivates such attacks.

Due to the controversial nature of aspects of the technology, LPR technology will continue to represent a potential target for hacktivist threat actors.

Although there was limited intelligence found on dark web and clearnet forums in relation to planned cyber-attacks and vulnerability exploitation in LPR technology, we judge that forums will highly likely continue to attract threat actors interested in IoT technology and the industry's technological advancements.

ARMED WITH INSIGHT

CONFRONTING TODAY'S CYBER CHALLENGES WITH CONFIDENCE

As we round the corner of the second year of the COVID-19 pandemic, public safety systems and data are becoming increasingly integrated, creating new challenges for security teams as they defend against criminals, nation-states, hacktivists and others.

These bad actors know that dependable, secure emergency services are essential to combat the pandemic and keep citizens safe from other everyday dangers. That is what makes them such enticing targets.

Our hope is that the knowledge contained in this report empowers public safety organizations to fight back with actionable insight into the methods, aims and operations of adversaries.

Today, this knowledge is a core building block of every product and service Motorola Solutions offers. Our customers face increasingly sophisticated and dangerous cyber threats.

Yet, they are not facing this threat alone. Armed with insights such as those found in the Motorola Solutions 2021 Cyber Threats to Public Safety report, they can confront today's cyber challenges with confidence.

GLOSSARY OF TERMS

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

- **Administrative lines:** Specific ingress phone numbers belonging to PSAPs (such as 1-800 numbers). These lines exist in addition to emergency lines used for 9-1-1 call routing.
- **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 Telephony Denial of Service attacks.
- **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.
- **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.
- **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.
- **Telephony Denial of Service:** A Telephony Denial of Service (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.

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. A "high confidence" judgment is not a fact or a certainty, however, 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.
- **Low Confidence:** Generally means questionable or implausible information was used, the information is too fragmented or poorly corroborated to make solid analytic inferences, or significant concerns or problems with sources existed.

SOURCES

[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] Someone who lacks networking and programming knowledge, and who uses existing software to launch an attack. Often a script kiddie will use these programs without even knowing how they work or what they do.

[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] See attack.mitre.org for more detail.

[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] A system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

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

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

MOTOROLA SOLUTIONS

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