if (this.readyState == 4 && this.status == 200) {
document.getElementById("demo").innerHTML = this.responseText
}
xmlhttp.onreadystatechange = function() {
if (this.readyState == 4 && this.status == 200) {

2022 CYBER THREATS TO PUBLIC SAFETY

UNDERSTANDING THE GLOBAL IMPACT OF WAR, DISRUPTIONS AND SUPPLY CHAIN CHALLENGES

Insights from the Motorola Solutions Threat Intelligence Team

Since 2018, the Motorola Solutions Threat Intelligence Team has compiled annual research and insights into the cyber threats facing first responders and public safety organizations around the world.

In 2022, the world became more adept at living with COVID-19 and cautiously began returning to a sense of normalcy. Yet, public safety, like other sectors, still grappled with critical disruptions, including continued supply chain challenges and Russia's invasion of Ukraine.

In this year's annual report, we share our findings on how these trends and events have impacted cyber-criminal organizations, hacktivists and other threat actors. We also examine the adversaries who target public safety and their tactics, techniques and procedures (TTPs).

To compile this report, the Threat Intelligence Team used proprietary, anonymized data along with publicly reported and closed source cyber intelligence from January 1 – December 31, 2022. We also applied comprehensive research into the public safety technology space including information from criminal forums, trusted vendors and government reporting to identify the most pressing and significant threats, threat actors and risks. We used numerous intelligence analysis techniques in the assessment of threat intelligence provided in this report.

2022: THE YEAR IN PUBLIC SAFETY CYBERATTACKS

Last year, cyberattacks on public safety were greatly influenced by the aftereffects of the Russian invasion of Ukraine. The conflict created a global cyber battleground among a highly-resourced and capable coalition of cyber forces composed of official nation-state armies and grassroots militias established to defend their respective homelands.

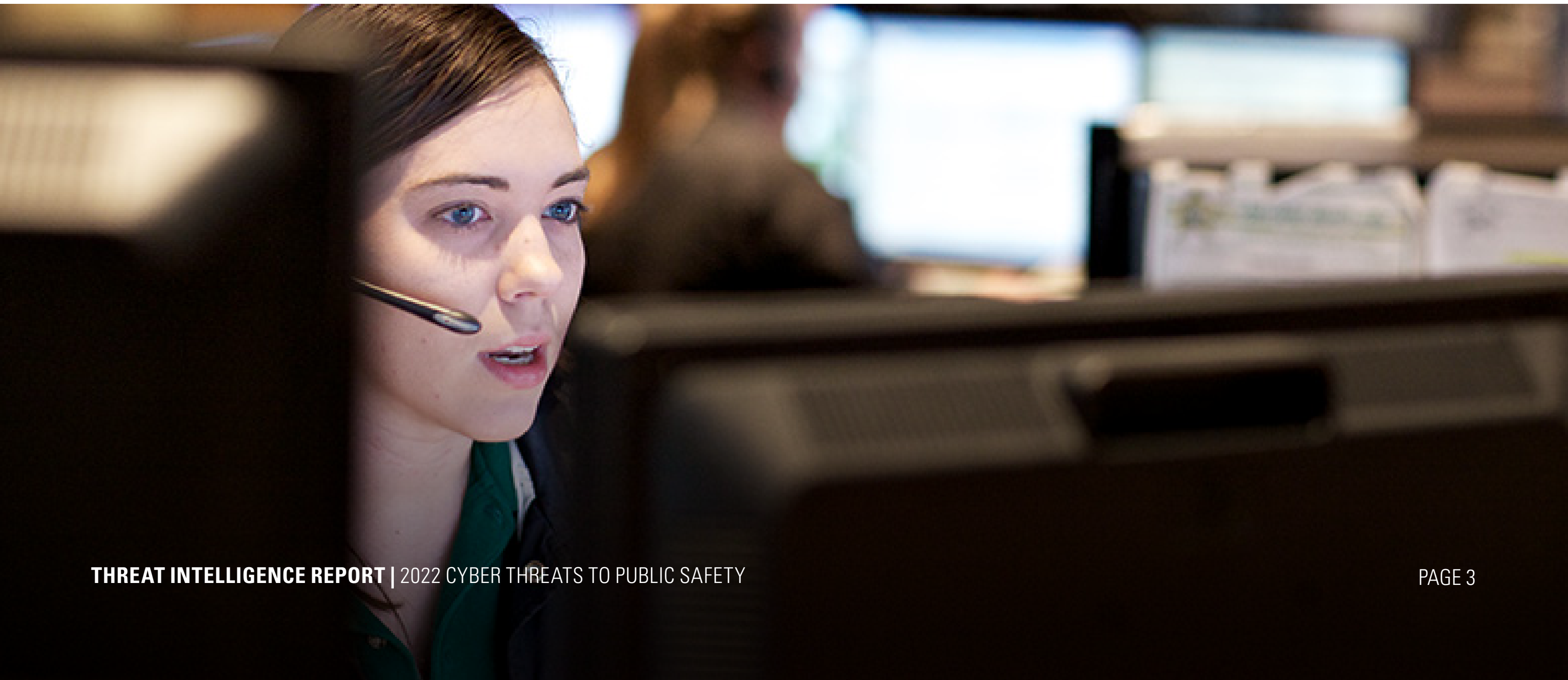
Pro-Russian hacktivist groups, established in response to the war in Ukraine, significantly increased the likelihood of attacks to public safety organizations through their highly-persistent, yet low impact distributed denial-of-service attacks (DDoS) and website defacements. Their frequent targeting of government agencies in nations friendly to Ukraine spurred a 179 percent increase in hacktivist activity against public safety agencies compared to 2021. As a result, 2022 saw a 700 percent increase in DDoS attacks to public safety organizations, almost all from pro-Russian hacktivists.

As a result of the operational and economic fallout from the war, there was an overall rise in cyberattacks to public safety in the past year, increasing from an average of 17 attacks per month in 2021 to almost 19 in 2022.

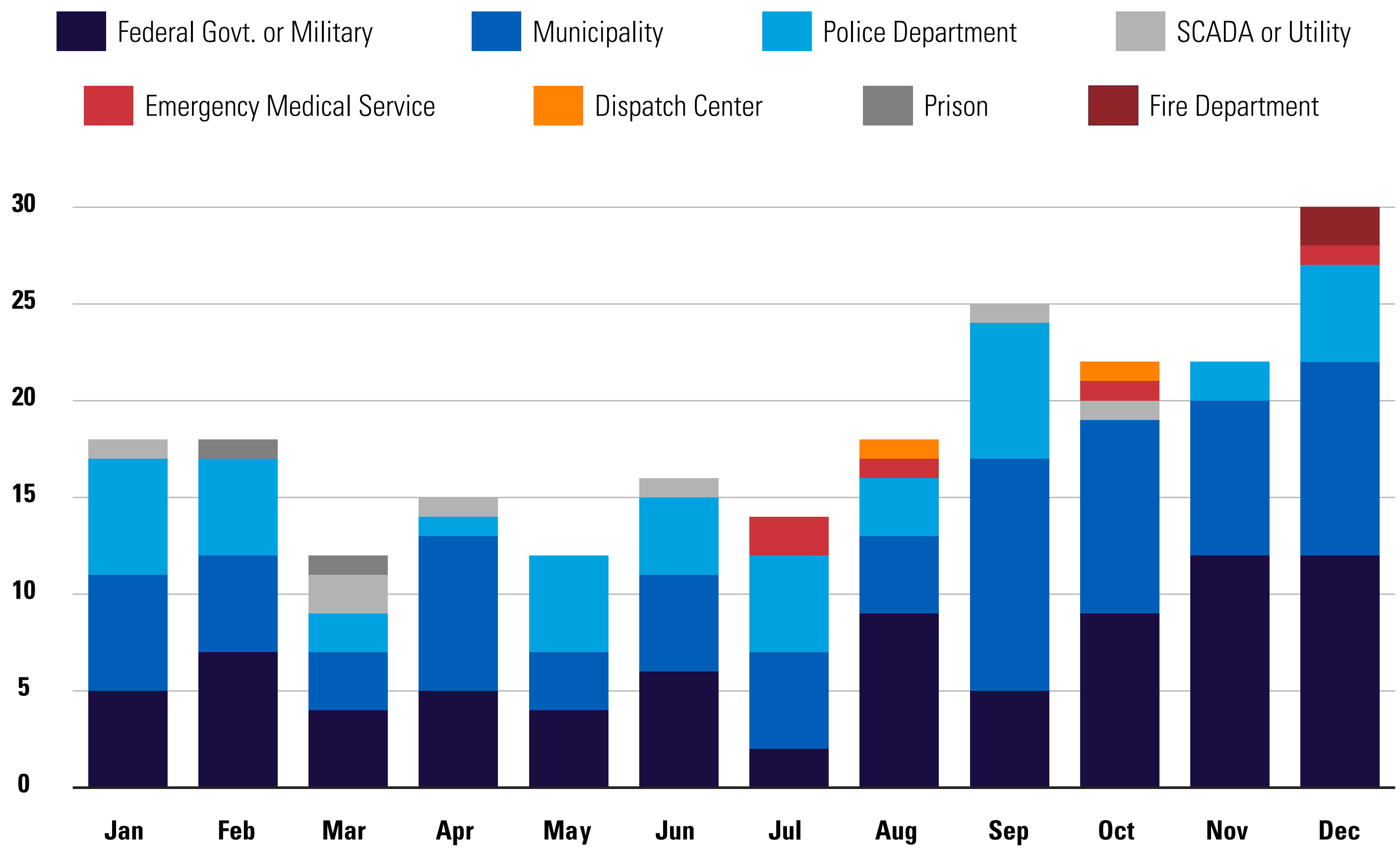
Year	2019	2020	2021	2022
Number of Cyber Attacks (% change from prior year)	**154**	**126** (-18%)	**199** (+58%)	**225** (+13%)

Quarter	Q1 2022	Q2 2022	Q3 2022	Q4 2022
Number of Cyber Attacks (% change from prior quarter)	**46**	**44** (-4%)	**58** (+32%)	**77** (+33%)

Across all public safety industries, the only area that saw an increase in attacks was the federal law enforcement space, which jumped from an average of two attacks per month to four. This was a direct result of national assets being targeted as retaliation for, or against, the invasion of Ukraine.



2022 CYBER ATTACKS TO MISSION CRITICAL SYSTEMS



Cybercriminals remained the top threat to public safety in 2022 overall, targeting a range of entities that included law enforcement agencies, SCADA deployments in public utilities and municipalities. In Q1 2022, we observed a decline in ransomware activity due to disruptions to criminal infrastructure and cash flow operations caused by the Russia/ Ukraine war's sanctions. However, by Q2 and Q3, extortion attacks returned to their previous frequency of around seven attacks per month against public safety, as groups expanded and refined their capabilities.

The cybercriminal community underwent significant transformation in 2022, which also caused a temporary drop in the frequency of attacks. Criminal gangs reorganized, acquired new servers, domains and other infrastructure, updated operational practices and introduced new selling points such as modular malware and increased profit sharing to attract top crime affiliates.

The only attack motivations to increase in 2022 were hacktivism and acts of war, which were connected to the observed spike in federal attacks. Hacktivism, the second-most prominent threat to public safety, saw the most development leading up to the midpoint of 2022. Loosely assembled 'hacktivist collectives' became more organized under focused causes, particularly the war in Ukraine. This allowed hacktivist threat actors to increase their capabilities with help from prominent cybercriminals who offered their assistance to respective pro-Western or pro-Russian causes.

This increased sophistication and collaboration resulted in 29 hacktivist attacks targeting sensitive databases to leak and expose, as well as shut down, internet-facing and internal systems. Of the known hacktivist attacks in 2022, 62 percent targeted federal public safety organizations while the remaining 38 percent focused on local law enforcement. The latter occurred in response to civil unrest, which is consistent with our observations in previous reports.

THREAT ACTOR DEVELOPMENTS

The LockBit extortion syndicate seemed to diminish as 2022 progressed. While they did attack three public safety entities in Q4, this was well below their normal attack cadence of seven per quarter. The lower attack cadence may be attributed to the arrest of Mikhail Vasiliev[1] on 10 November 2022, an alleged LockBit associate. Another potential cause for a drop in attacks may be that their ransomware builder became public, which allowed a more in-depth view of their encryption method[2]. The builder consists of all the files necessary to create and launch the LockBit 3.0[3] ransomware.

BlackCat and Hive were also top extortion syndicates in 2022, both with four attacks in Q4. In Q1 – Q3, Hive averaged one attack and BlackCat averaged two attacks on public safety targets. The increase in public safety targeting by Hive and BlackCat may be attributed to the void left by LockBit not targeting public safety as frequently in Q4.

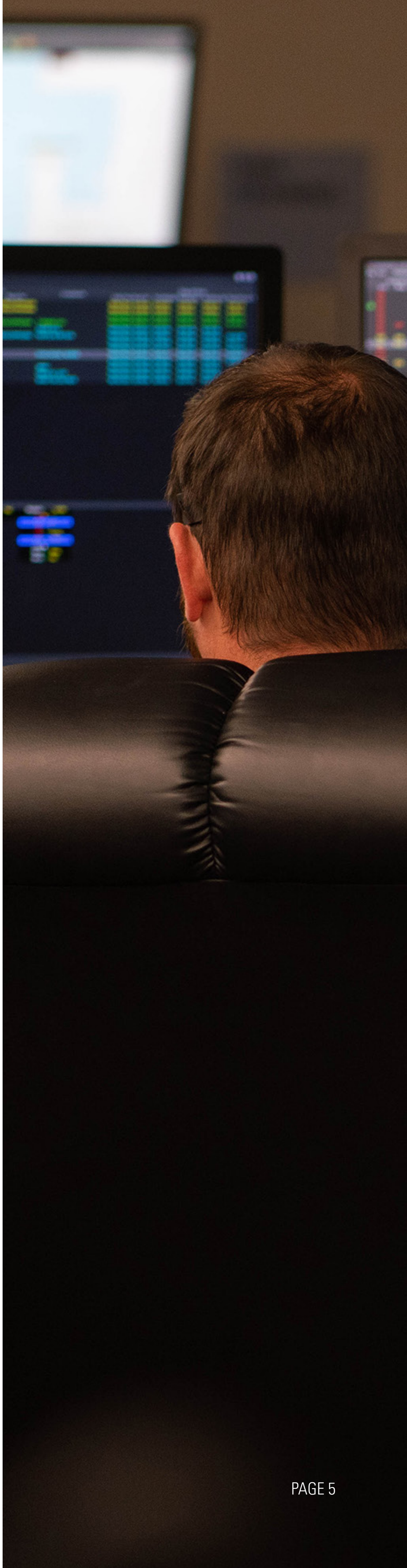
Russian hacktivists also played a major role in late 2022 as noted above. Unlike past quarters where KillNet solely performed DDoS attacks against Ukrainian sympathizers, in Q4 several other hacktivists groups joined the cause. XakNet, Anonymous Russia and NoName057(16) all performed multiple DDoS attacks against public safety systems.

The Royal extortion syndicate[4] also quickly rose to prominence in late 2022. Employed by several ex-Conti members, Royal was the most active extortion syndicate across all industries in November 2022. It is estimated Royal represented 16 percent of the extortion attacks globally in November, knocking LockBit from the top spot for the first time since September 2021[5]. Even though Royal did not attack any public safety targets in Q4, based on their current attack cadence and opportunistic target selection, it is likely they will attack one in the near future.

2023 OUTLOOK

Extortion cybercriminals are almost certainly going to expand operations and increase the sophistication of their attacks across all industries into 2023. Their targeting of public safety has remained largely opportunistic and that is expected to remain consistent; however, the growing cadence of overall attacks increases the likelihood of significant compromise to public safety operations. We have observed a growing number of groups willing to extort public safety organizations throughout 2022, which is expected to continue into 2023 as well.

While Russia and Ukraine are still in the midst of conflict, pro-Russian hacktivist activity against public safety targets will likely continue. The attack cadence for these groups is largely based on actions by NATO or Ukrainian sympathizer countries. While DDoS attacks and defacement of websites are low sophistication and low impact, pro-hacktivist groups will continue to launch these attacks to show their support for Russia in 2023.



APPENDIX A:

ASSESSMENT AND RESPONSE, STANDARD OPERATING PROCEDURES

LEVELS OF ANALYTIC CONFIDENCE

High Confidence	Moderate Confidence	Low 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.	Generally means credibly sourced and plausible information, but not of sufficient quality or corroboration to warrant a higher level of 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.

[1] https://www.justice.gov/opa/pr/man-charged-participation-lockbit-global-ransomware-campaign

[2] https://www.scmagazine.com/analysis/ransomware/royal-overtakes-lockbit-as-top-ransomware-in-november-as-attacks-increase-41

[3] https://www.hhs.gov/sites/default/files/lockbit-3-analyst-note.pdf

[4] https://www.cybereason.com/blog/royal-ransomware-analysis

[5] https://www.scmagazine.com/analysis/ransomware/royal-overtakes-lockbit-as-top-ransomware-in-november-as-attacks-increase-41

LEVELS OF ANALYTIC CONFIDENCE

Very High	High	Medium	Low
No patch available, exploit available and/or being actively exploited in the wild.	No patch available and proof-of-concept (POC) or exploit available for use. No threat actors observed actively exploiting this vulnerability.	Patch available and proof-of-concept (POC) or exploit available for use, or vulnerability is rated as critical.	Patch available and no proof-of-concept (POC) or exploit available.

For more information, visit
motorolasolutions.com/psta

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

The information, methodologies, data and opinions contained or reflected herein are proprietary of Motorola Solutions, Inc. (Motorola Solutions), except where ownership is expressly attributed to another party. They are provided for informational purposes only, intended for internal non-commercial use and may not be copied, distributed or used in any way, including via citation, unless otherwise explicitly agreed in writing. These are based on information made available by third parties, subject to continuous change and therefore are not warranted as to their merchantability, completeness, accuracy or fitness for a particular purpose. Any representation or warranty that might be otherwise implied is expressly disclaimed. The information and data are provided "as is" and reflect Motorola Solutions' opinion at the date of their publication and Motorola Solutions has no obligation to update them. Motorola Solutions does not accept any liability for damage arising from the use of the information, data or opinions contained herein, in any manner whatsoever, except where explicitly required by law. Any reference to third party names or third party data is for appropriate acknowledgement of their ownership and does not constitute a sponsorship or endorsement by such owner.