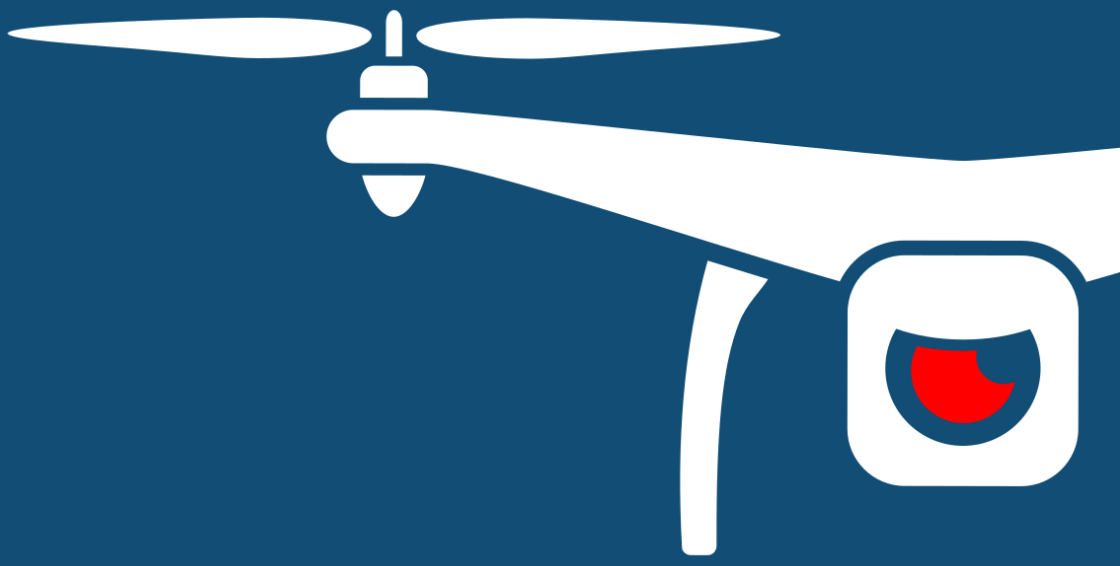
DRONE SEC
A Privasec COMPANY

NOTIFY ISSUE #1

WEEKLY THREAT INTELLIGENCE

19 December 2019 | v1.0 RELEASE



UAS HACKING, HARDENING AND DEFENCE

UAS PENETRATION TESTING
COUNTER-UAS CONSULTING
FORENSICS & INCIDENT RESPONSE
AERIAL THREAT SIMULATIONS
DRONE SECURITY MANAGEMENT PROGRAMS

DOCUMENT **CONTROL**

PREPARATION

DroneSec (dronesec.com)

Threat Intelligence Team

Email: info@dronesec.com

Phone: 1800 996 001 | + 614 7854 3434 (Urgent)

EXECUTIVE SUMMARY

This document covers the playbook and methodology for Drone, Counter-Drone and UTM Security and Threat Intelligence reports. We use a variety of sources[1] to aggregate, assess and analyse relevant information that can be used to fine-tune counter-drone measures, provide concrete evidence towards drone security business cases and uplift our own consultants' skills and abilities.

In this first public edition of DroneSec Notify, you may be thinking "how does this apply to me?" We've been dedicated to bringing drone security news and events to the public since 2016 via dronesec.xyz. Over the past few years, we focused on tailored intelligence that followed a simple principle – important and actionable. So far, this intelligence was provided only to select organisations and partners.

Recently, we've been refining our methodology, expanding our sources and improving the time we get intelligence notifications out to those who need it most. Our position of being deeply embedded in the Information Security community, utilising the resources available to us through Privasec and having over 100 years combined experience in the Threat Intelligence and Incident Response industry is a testament to our ability to provide important, actionable intelligence to vendors, governments and organisations around the globe.

We've been growing, and with it have acquired talented staff with experience of working in a variety of environments including the Department of Defence, Air Force, BAE Systems, DXC, Sense of Security and many more. Our staff have co-authored documents published by the Australian Government on security hygiene, used drones in Red Team and Aerial Threat Simulations against national Critical Infrastructure (SCADA/ICS) and tracked down malicious actors causing disruption to government departments. In short – we're serious about security and are here for you.

We have clients in different stages of their journey into drone security. Some are considering technologies to protect their environments, others building software to support drones and yet others using COTS[2] drones to improve efficiency in their individual sectors. No matter the stage, our intelligence aims to uplift the security posture of their drone programs. We've experienced the highs and lows – intelligence too late, but other times information that has enabled businesses to make key decisions pre-emptively; earning the trust of their stakeholders and technical teams.

We're now at a stage in our own journey where we're able to support the specific needs of more organisations. As a result, we're extending our intelligence reports to a select pool of subscribers where they can get a taste of what we provide to our priority, paid partners in the Notify platform. I hope the reports continue to provide strategic information to your drone program and we look forward to sharing more developments with you in the future.

- *Mike Monnik, DroneSec CTO*

[1] List of sources can be found in Appendix A.
[2] COTS: Commercial-Off-The-Shelf (readily purchased by the public)

TABLE OF **CONTENTS**

1. THREAT INTELLIGENCE

1.1. INTRODUCTION

Threat Intelligence to the DroneSec team means cutting-edge information, news, resources and threats delivered in a succinct and actionable way. Notify is just that – key information that can be used to prepare, prevent and identify threats and challenges which seek to take advantage of the drone industry. Our aim is to allow organisations to make more informed decisions, respond effectively and get a birds-eye view of our core focus: Drones, Counter-Drone and Universal Traffic Management (UTM) Systems – also referred to as **DCU**.

When it comes to proactively seeking out the best solutions, developing response capabilities or building resilience into your drone operations, relevant information is king. We're dedicated to ensuring you stay up to date through Notify, while getting the specific details around techniques, vulnerabilities, targets and malicious actors. Furthermore, we've made all Notify information both scalable and easily categorised, providing a mechanism for easy search but also extraction of statistics and use cases for stakeholders who need pre-mitigation insights and strategies.

For technical operators, we've included the ability to be able to prioritise relevance over noise and communicate with each other to exchange ideas and collaborate on threats. This exchange happens on a number of levels, from our slack channel, to sharing DroneSec case-studies within the platform and hearing from our partners (individuals, technology vendors, law enforcement and regulatory bodies) who supply valuable information to Notify.

Weekly reports are just that – the lifespan only covers one week of intelligence and where this might extend is when we detected or were alerted to it later on. You can rely on this information not being too old or outdated; but you're always able to browse the archives and library for older artefacts. Anything breaking news, we send off immediately to our Notify subscribers – outside of this, the report covers the rest on a weekly basis.

So how does it all work? To view our methodology, sources and scoring matrix, head down to the appendices to get a feel for it all. Otherwise, information we deem as being 'key' is featured with insights and analysis supplied for reader's benefit. The rest of the information we pick up that can be categorised as security-based intelligence for DCU is placed thereafter. Our categorisation and tagging system mean that on a monthly basis, you'll get an overview of the statistics we've seen – updated in real-time, week-on-week for pattern recognition analysis.

Kicking it all off, we're delivering our first round in a PDF format. In the next few weeks, we'll continue to roll out platform access to ensure we can sustainably support our current client needs with relevant, actionable information within the context of DCU.

Something we missed? Keen to become a supplier? Want to join the Notify platform? Shoot us a message at info@dronesec.com. Otherwise, feel free to hop into the slack channel and introduce yourself: DroneSec Slack Channel.

1.2. FEATURED ADVISORIES

The prioritisation table and its dependencies are explained in Appendix A, and relate to how we filter, analyse and visualise the intelligence we collect.

Exploits and Vulnerabilities	Tags	Priority
DroneSploit Exploit Kit for Drones Released	Drones, Cyber Security	P2

First observed 5/12/19 – Status: UNKNOWN

Summary

A dedicated exploit framework has been released comprising of various drone hacking techniques.

Overview

The framework consists of both old and new attack vectors against a variety of drone types, including passive and active monitoring, deauth[3] attacks and vectors to break into closed drone-controller circuits. The aim is to automate and streamline the process, being simple to conduct and visualise the results in real-time.

The framework is limited in its ability to only target WiFi-based drones (e.g. AR Drone, DJI Tello, Mavic Mini) but not RF-based drones (DJI Phantom 4, Mavic Pro etc) but the goal being to bring together as many exploits as possible for drones under one roof. By typically Information Security standards, it seeks to make users aware of the risks and perform simulated attacks against their own systems in order to better protect them.

DroneSec Analysis

DroneSec conducted tests on four drone systems using the DroneSploit framework. Video release and dedicated writeup to follow.

Recommendations

As with any WiFi-based drone systems, ensure appropriate attack-vectors have been identified and simulated against. For drones that allow modification of their Wireless Access Points (WAPs) and associated passwords, customise these before flight operations, disable open-connectivity and ensure networks are protected with up-to-date encryption standards. Where possible, use MAC filtering to ensure only your trusted devices can connect. Review your drones' action-policy for what happens when it loses connectivity and document the process for any unexpected actions it might take.

References:

https://github.com/dhondta/dronesploit

https://github.com/dhondta/dronesploit/blob/master/docs/blackhat-eu19-arsenal.pdf

https://portswigger.net/daily-swig/black-hat-europe-new-tool-offers-metasploit-like-framework-for-hacking-into-drones

Affected System(s):

```
WiFi-based Commercial-Off-The-Shelf drones
```

Exploits and Vulnerabilities	Tags	Priority
Drone Data-Analysis Applications Expose Critical Drone Data	Drones, Cyber Security	P2

First observed 11/12/19 – Status: DRONESENSE INSTANCE PATCHED, EXPLOITABLE IN THE WILD

[3] Deauth: De-authenticate – A number of packets sent to the controller or drone to separate the connection and allow the opportunity of a new device to connect and take place.

Summary

Sensitive drone flight path, owner and details leaked via traditional web application security misconfigurations. On this instance, a public report reveals DroneSense' telemetry and flight data were left accessible on a cloud-storage system, which detailed Law Enforcement and Government operations and flight logs.

Overview

DroneSense, an organisation that provides a platform for several government, law enforcement and private clients to fly drones and manage their data, exposed a database of information due to a misconfigured security storage system. Flight path data, brand of drones, names and email addresses, and other technical information about the drones were in the database, however, no camera footage was included in the leak.

The myriad of information gives insight to how businesses and government agencies such as law enforcement and safety services are using drones as part of their operations such as search and rescue or to locate and survey people. The data shows nearly over 200 different entities.

The information leak could mean the loss of data privacy and potentially, the general security expectations of law enforcement could very well undermine investigations or the justice process.

DroneSec Analysis

In 2019 alone, DroneSec made 6 critical-level discoveries of information within drone-data analysis software and web applications, leading to disclosure of the following artefacts:

- Being able to see private flights, thumbnails and personal information of the drone owners;
- Being able to see flights being stored for legal processing in court cases;
- Being able to discover lists of drone purchases by different entities and law enforcement organisations (make, model, type); and,
- Being able to manipulate and modify flights by others recorded in these 'flight ingest system' software sites.

There's a huge initiative on the innovation of being able to record, visualise and post-analyse drone flights, with not very much focus on the security element of it all. Without naming them, we've found a number of these organisations storing this data in open Amazon S3 buckets, Azure Storage blobs and Aliyuncs (Alibaba Cloud) storage buckets. This isn't new – the Department 13[4] team (namely Kevin Finisterre) has located various encryption and control data within GitHub repositories and Amazon S3 buckets – with available resources such as GreyHatWarfare[5] and Dehashed,[6] it's becoming significantly easier to discover these data leaks with ease.

By not properly protecting private flights or storing flight records (and key indicators such as Remote ID's), traditional cyber security vulnerabilities that are now passed onto drones. In some of the worse cases, software that can control a number of drones at once (UTM systems) could be hacked into and not just result in server or root access, but remote access to drones' mid-flight. This becomes increasingly relevant as the Information Security and Drone/Aviation industries continue to merge.

The vendors that DroneSec have worked with have identified and patched these vulnerabilities within < 6 weeks. Some of those vendors now contribute and exchange threat information to Notify. Redacted use cases and Proof-of-Concept findings can be found within the Notify Portal to further uplift organisations development posture.

Recommendations

DroneSense is one of many platforms that provide drone flight-data analysis. Any software (or associated infrastructure) your organisation is using in its drone program should undergo security checks or penetration tests. More specifically, this should occur with the perspective of a simulated attacker seeking to chain attacks from traditional computer systems and communication protocols to a hybrid of drone data and if applicable, control.

[4] Company: https://department13.com/ Report: http://www.digitalmunition.com/WhyIWalkedFrom3k.pdf
[5] GreyHatWarfare (AWS open S3 bucket explorer): https://buckets.grayhatwarfare.com/
[6] Dehashed (Leaked Database/Breached Credentials Explorer): http://dehashed.com/

Organisations should have a register of what data is: (1) meant to be private and/or encrypted, (2) protected by data sovereignty rules, and have (3) a process for removing or redacting sensitive information stored on third-party systems and (4) an incident response plan or SOP[7] in the event sensitive drone-related data are leaked. These are key questions to ask your drone flight-data software or application vendors before onboarding or exchanging information between your unmanned assets and their storage systems.

References

https://www.vice.com/en_us/article/qjdddp/data-shows-where-police-fly-drones-dronesense

Affected System(s)

```
Public, private and Law Enforcement/Government users of DroneSense
```

Exploits and Vulnerabilities	Tags	Priority
Spoofing the DJI AeroScope Counter-UAS System Proof-of-Concept	Drones, Cyber Security, All Sectors	P2

First observed 23/02/19 – Status: UNKNOWN

Summary

An individual with access to DJI's AeroScope drone-detection and response portable system has managed to spoof the simulated location of multiple 'rogue' drones by rapid injection of randomised DroneID entities. This results in locking up the AeroScope's interface, rendering it unusable. Tools have been made available online.

Overview

DJI AeroScope is a drone detection monitoring platform that identifies UAV communication links and gathers data such as flight status, paths and other information real time. The device is able to provide central monitoring and playback from past data collated.

Kevin Finisterre was able to trick the system by using adjusting modules that allowed him to spoof the DroneID which are essential for DJI AeroScope to monitor drones.

DroneSec Analysis

The DJI AeroScope system is a drone-vendor response to being able to detect popular DJI drones in the market today. It has been used by aviation authorities, correctional facilities and some airport locations for detecting the number of drones in the area. However, it is well known that potential attackers or disruptors have and can use custom drone or less popular commercial drones (or on different frequency bands) to avoid detection. Electronic or information-security based vectors of spoofing or DoS[8] are a realistic scenario for these systems and should be considered before providing to critical environments and law enforcement agencies.

Bypasses aren't just electronic however - ISIS has managed to modify commercial drones with the capability to carry explosive payloads, proving lethal to the U.S. armed forces. Lawmakers can bill regulations to ensure that drones are registered, however, like any lone wolf attacks or organised syndicated crimes, such regulations would not be sufficient to prevent modified or custom drones.

In 2017, DroneSec conducted a workshop for attendees to detect drones by their MAC address embedded within the drone and their controllers' Wireless Access Points. Usually easy to identify, it only took a couple of Raspberry Pi's to generate a number of fake SSID's and spoofed MAC addresses to confuse participants using wireless enumeration tools. This represented a loss in accurate decision-making as to which wireless signal belonged to a legitimate drone versus that of a static, small embedded computer system.

For Counter-UAS vendors, extending their roadmap to various "emerging threats" such as swarms or spoofing should be key – the obvious choice of a malicious drone user will be to disable, confuse or bypass Counter-

[7] SOP: Standard Operating Procedure

[8] DoS: Denial-of-Service, the ability to flood a system with too many communications, rendering it inoperable.

UAS systems that might represent a threat to their nefarious activities.

Recommendations

Organisations creating Counter-UAS equipment should have their systems tested against traditional cyber-security attack vectors. Penetration testing, red teaming and risk profiling should be involved in the development phase to prevent the Counter systems from being countered themselves.

For aviation authorities or organisations using the AeroScope system, particularly those depending on them to provide accurate statistics and early-warning for critical sites, consider getting third-party assurance on vendor-based Counter-Drone systems before utilising in your environment. This is as true for potential bypasses as it is for information received, stored and transmitted by the product to internet-based or 3rd party systems.

For DJI, it's a case of unfortunately not performing adequate technical assurance on their system before providing it to the market, and now looking to patch or release an update (if even possible) to combat the method used against it.

References

https://www.youtube.com/watch?v=EdRvaTlKJIA

https://github.com/rapid7/metasploit-framework/pull/9301

https://github.com/DJISDKUser/metasploit-framework/commit/4682525f176861d1cb68bf006ff0afe0a3ab5617

Affected System(s)

```
DJI, Private and Government users of the DJI AeroScope system
```

1.3. NEWS AND EVENTS (P3)

Gang uses Drones to Drop Bird-Flu Infected Items into Pig Pens to Influence Sell Price

Gangs spread rumours about the African swine fever and use drones to drop infected items into farms in bid to get farmers to sell their pigs at a low price before smuggling the meat and selling it on as healthy stock. (https://supchina.com/2019/12/16/the-chinese-gangsters-using-drones-to-spread-african-swine-fever/)

Transport Security Authority (TSA) queries Airports to Use Counter-UAS Against Rogue Drones

TSA wants to give air marshals the power to use Department of Defence equipment to shoot down drones near airports, seeking to tackle drones that can disrupt airport operations. (https://www.securitymagazine.com/articles/91399-tsa-wants-to-shoot-down-drones-near-airports)

UK Plans to Enable Authorised Private Sectors to Use Counter-UAS Systems

The British Government plans to expand the list of authorised private sectors to take drones out of the sky outside from the initial police and armed forces. (https://www.telegraph.co.uk/sport/2019/10/22/exclusive-british-sports-venues-could-given-power-disrupt-drone/)

Marine Corps Commandant Highlights New Tactical Unmanned Systems Needs

General David H. Berger of the U.S. Marine Corps has, in testing with various wargames and research topics to match the National Défense Strategy, called on new operations including small tactical unmanned aircraft systems along with electronic warfare measures. (https://warontherocks.com/2019/12/notes-on-designing-the-marine-corps-of-the-future/)

1.4. NEWS AND EVENTS (P4)

UK Airprox Board Investigates Serious Collision Risk Incident Between Drone and Luxury Jet

https://www.mirror.co.uk/news/uk-news/drone-comes-within-10ft-crashing-21110782

Japanese Coast Guard to Stop Using Drones from Chinese-Origin Vendors

https://asia.nikkei.com/Politics/International-relations/Japan-Coast-Guard-to-eliminate-Chinese-drones

Photographer Arrested in Hong Kong after Drone Falls into Chinese-Owned Barracks

https://www.scmp.com/news/hong-kong/law-and-crime/article/3041894/photographer-arrested-losing-control-drone-camera-fell

Seized SD-Card Shows On-Board Video of Drone Dropping Contraband into Dublin Prison

https://www.thesun.ie/news/4871154/footage-drone-drugs-dublin-prison/

Seven Drones Disabled by Droneshield Counter-UAS Technology at SEA Games

https://www.shephardmedia.com/news/uv-online/droneshield-systems-protect-southeast-asian-games/

Drone Transmitting Images to Police Headquarters Falls on Apartment Roof in Athens, Greece

http://www.ekathimerini.com/247133/article/ekathimerini/news/police-drone-falls-on-roof-of-athens-apartment-building

Ireland Lacking Education, Regulations, Equipment and Countermeasures Against Drones

https://www.irishtimes.com/news/environment/military-and-garda-ill-prepared-for-drone-threat-says-report-1.4109913?mode=amp

French Port Actively Utilising Real-Time Autonomous Drone Security Systems

https://dronelife.com/2019/12/16/dronelife-exclusive-azur-drones-this-security-guard-is-on-duty-24-7-patrolling-dunkirk-port/

Counter-Drone Market to Grow Extensively Within Decade

https://www.theguardian.com/news/2019/dec/12/detectors-jammers-and-cyber-attackers-the-rise-of-anti-drone-tech

Armed Drone Attached with Machine-Gun for Use in Turkish Military Forces

https://www.newscientist.com/article/2227168-turkey-is-getting-military-drones-armed-with-machine-guns/#ixzz68RpS8yZh (https://www.youtube.com/watch?v=obyuBeixIM8)

Turkey to Use Autonomous Drone Swarms in Combat Within Syria

https://www.newscientist.com/article/2217171-autonomous-killer-drones-set-to-be-used-by-turkey-in-syria/ (https://www.youtube.com/watch?v=3d28APIfwSI)

Drone Swarms Clutter Radar Systems, Confuse Sensors and Attack Russia's Khmeimim Airbase

https://www.theguardian.com/news/2019/dec/04/are-drone-swarms-the-future-of-aerial-warfare

1.5. COUNTER-DRONE SYSTEMS (P4)

Journalistic Review of Various C-UAS Systems, Types and Technologies

https://www.theguardian.com/news/2019/dec/12/detectors-jammers-and-cyber-attackers-the-rise-of-anti-drone-tech

U.S. DoD Releases "C-UAS Strategy" Document and Financial Results for 2019

https://gcn.com/articles/2019/12/11/counter-uas.aspx

Kongsberg Defence & Aerospace Secures C-UAS Contract with German Armed Forces

https://www.army-technology.com/news/kongsberg-c-uas-german-armed-forces/

FALKE Project Funded to Deploy C-UAS in Airport Environments by German Transport Minister

https://www.internationalairportreview.com/news/108888/project-falke-counter-drone-system-development-gains-funding/

Spanish MOD Select Aeronautica's Hand-Held Drone Guns as C-UAS and C-Swarm Technology

https://www.unmannedsystemstechnology.com/2019/12/spanish-ministry-of-defense-selects-portable-counter-drone-systems/

Pentagon Positions C-UAS Strategies and Technologies as Key Priority for U.S. DoD In 2020

https://www.c4isrnet.com/unmanned/2019/12/11/pentagon-wants-to-streamline-its-counterdrone-focus/

Preventing Emerging Threats Act Spurs on C-UAS Vendors in Massive Threat Escalation

https://www.securityinfowatch.com/perimeter-security/robotics/anti-drone-technologies/article/21114729/counterdrone-tech

Altitude Angel and Heliguy Join Forces to Develop Joint-UTM/Counter-UAS System

https://www.commercialdroneprofessional.com/operation-zenith-collaboration-comes-together-as-altitude-angel-and-heliguy-team-up/

1.6. WHITEPAPERS AND PUBLICATIONS (P4)

Counter-Drone Systems 2nd Edition – Dronecenter @ Bard College

https://dronecenter.bard.edu/projects/counter-drone-systems-project/counter-drone-systems-2nd-edition/

Policy Paper: UK Counter-Unmanned Aircraft Strategy

https://www.gov.uk/government/publications/uk-counter-unmanned-aircraft-strategy

The U.S. Department of Defence' C-UAS Strategy Document

https://plsadaptive.s3.amazonaws.com/eco/files/event_content/c-uas-drone-strategy-2020In2BZvhXiRYdnFc71AUKfvCDMw1WHxcCGNvxIzN2.pdf

Thesis: A Game of Drones, Cyber Security in UAVs (Using STRIDE Model)

http://kth.diva-portal.org/smash/get/diva2:1350857/FULLTEXT01.pdf

Cyber Physical Security of Time-Critical UAV Applications (Maths Heavy)

https://arxiv.org/pdf/1902.03506.pdf

Cleared to Land: Pilot Visual Detection of Small Unmanned Aircraft During Final Approach

https://commons.erau.edu/ijaaa/vol6/iss5/12/

Internet of Things Forensics: Advances, Taxonomy, Requirements and Challenges

https://www.sciencedirect.com/science/article/pii/S0167739X18315644?via%3Dihub (Contact DroneSec for PDF)

Machine Learning for Wireless Connectivity and Security of Cellular-Connected UAVs

https://ieeexplore.ieee.org/document/8641422 (Contact DroneSec for PDF)

Risk Assessment of SDR-Based Attacks within UAVs

https://ieeexplore.ieee.org/document/8877144 (Contact DroneSec for PDF)

RPAS Forensic Validation Analysis Towards a Technical Investigation Process: A Case Study of Yuneec Typhoon H.

https://www.mendeley.com/catalogue/api/pdf/7cef5f22-0ddc-38e6-a056-baaf3fce7bf8/?doi=10.3390/s19153246 (Contact DroneSec for PDF)

Dronerf Dataset: A Dataset of Drones for RF-Based Detection, Classification and Identification

https://www.mendeley.com/catalogue/dronerf-dataset-dataset-drones-rfbased-detection-classification-identification/

International Standard ISO 2138403 Unmanned Aircraft Systems Released for Drones

https://www.iso.org/news/ref2461.html

Enjoy these resources? More papers/published articles come out in a week than we can put on a page. Let us know if this was useful and we'll provide backlog access to our knowledge base from 2014 – current.

APPENDIX A: THREAT NOTIFICATION MATRIX

A.1. OBJECTIVES

The sole focus of this service is to supply organisations with key evidence, alerts and intelligence relating to (1) Drones, (2) Counter-UAS and (3) Universal Traffic Management (UTM) systems. Together, these three items are referred to as: **DCU**. This intelligence provides a defensive net for early warning systems, fine-tuning systems based on trends and providing agencies with factual evidence in support of selecting or rejecting the need for counter-solutions. High priority will be given for the following artefacts:

- Unfolding situations or incidents relating to DCU;
- Private or public-based vulnerabilities, exploits or attack vectors affecting DCU;
- Global or national regulatory changes affecting DCU;
- Remarkable vendor or brand-specific news releases.

If an artefact is released that is considered the highest priority level (P1), Notify customers will receive an email alert linking them to the intelligence details located within their Notify portal account.

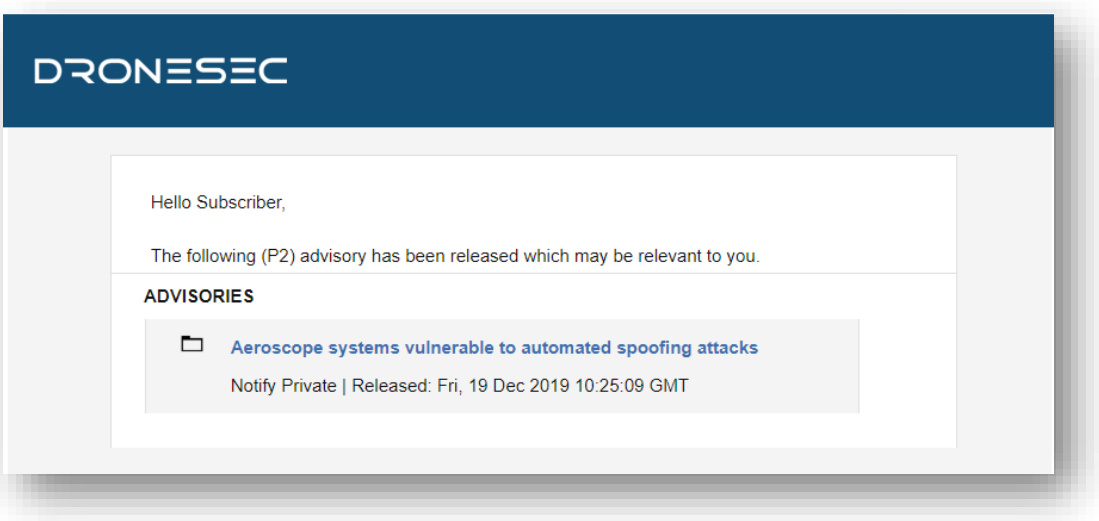


Figure 1 - A threat notification specific to a Notify customer's listed keywords.

DroneSec uses a methodology to rank, prioritise and filter intelligence pieces. This rating merges threat intelligence standards with the type of source (public, private, underground) and affected system (DCU).

Threat notifications are prioritised based on the following table:

Priority Level	Description
P1	Directly specific to a Notify customer
P2	High importance incident or situation
P3	Medium importance event or information
P4	Low interest or general news/media
P5	No direct evidence, market trends or informational

In general, (P1) alerts will only be visible to the affected customer to protect their privacy and general information security. However, abstract (P1) information will at times be shared with other Notify customers. Priority levels are often highly contentious as it requires understanding of a customer's environment, context and what might be deemed 'actionable' for them. The added spanner in the works is that DCU is made up of cyber-physical systems – there are traditional security vulnerabilities, physical and kinetic risks and even privacy, regulatory and aviation considerations in play. As a result, we set the priority level based on a number of key metrics that are very specific to our Notify customers; the more information provided about an entity, the higher the quality-gate of prioritisation we apply to our filter process.

Associated with each artefact of intelligence, you'll find a set of tags. These tags are used for indexing, searching and quickly visualising if the information is relevant to your organisation. As with any system, ours will continue to better itself as it learns more about the various artefacts that are most important to our customers, and their types of environments and systems. You'll find the tags, and examples of them, in the tables below.

There are three categories we focus on. We do not extend past these, as to keep our intelligence relevant and brief.

Tag - Categories	Description
Drones	Custom-made or Commercial-Off-The-Shelf (COTS) systems that might: • Be known as UAS[9], UAV[10], RPAS[11]… • Weigh 50g all the way to 250kgs • Are automated or manually piloted • Have associated devices, software or infrastructure
CUAS	Counter-UAS systems that might: • Be known as Counter-Drone or C-UAV

[9] UAS: Unmanned Aerial System
[10] UAV: Unmanned Aerial Vehicle
[11] RPAS: Remotely Piloted Aerial System

	• Detect and/or respond to drones • Be standalone, hand-held, static or integrated with a UTM[12] or PSIM[13] system • Have associated systems, software, infrastructure and communication protocols
UTM	Universal Traffic Management system that might: • Be known as Urban Air Mobility (UAM) or fleet management systems • Manage, track, communicate with or interdict drones and/or drone swarms • Be software and/or hardware based • Have associated systems, software, infrastructure and communication protocols

Within DCU, there are many areas of concern. For those in a position of ingesting Threat Intelligence, these are the key concerns we have determined are relevant for the information we collect.

Tag – Areas of Concern	Description
Cyber Security	Technical attack vectors, risks, threats, vulnerabilities, guides, OSINT[14], exploits or zero-days[15]. This may also contain confidentiality, Privacy, Integrity and data sovereignty artefacts
Safety	Safety concerns related to assets, environments, persons or critical systems as a direct result of the artefact. This can be caused by physical, kinetic or electronic sources.
Regulatory	Global or national law or regulatory-based amendments, announcements or ordinance that affect DCU.

Sometimes the artefacts may cover a range of sectors. For organisations looking to filter out noise, this is a key tag that will help provide insight into their chosen sectors.

Tag – Affected Sector	Description
Residential	Houses, suburban areas and private property.
Commercial	Cities, major working areas and buildings

[12] UTM – Universal Traffic Management System
[13] PSIM – Physical Security Information Management System
[14] OSINT: Open-Source Intelligence from the public domain.
[15] Zero-day: Otherwise known as an 0day or unknown, unpatched vulnerability of which the vendor does not yet know exists.

Government	Government-managed locations
Critical Infrastructure & Security	Water, energy, docks, airports, prisons, transport, stadiums and military
All Sectors	The above sectors, combined

APPENDIX B: SOURCES & LIMITATIONS

B.1. INTELLIGENCE SOURCES

DroneSec uses a variety of government, military, law enforcement, vendor and citizen-based intelligence sources. Not all of these sources are public. Sources or artefacts that cannot be verified by a third-party are clearly marked.

Source Name	Description	Intelligence Type
International Aviation Authorities	Aviation authorities are the regulatory bodies for managing air and drone activities within a range of jurisdictions. Their level of access includes pilot, airport, airprox and public incident reports.	Statistics Incidents
Academic Sources & University Agreements	Keyword alerts on various academic portals and research agreements with Higher Education provide Notify with the latest journals and papers with a focus on DCU.	Research Papers Studies and Reports
Pilots – Commercial and Private Airlines	Pilots currently active in the commercial or private airline industry.	AirProx Reports Visual Identification Reports
Commercial Partnerships	Our partners in the military defence, commercial vendor and security industry exchange intelligence with Notify.	Statistics Incidents Sentiment and chatter Vulnerabilities and Exploits
Counter-UAS vendors	Counter-UAS vendors with multiple systems in place around the globe. Their systems detect, record and (where allowed) react to malicious drones. Detection telemetry data is shared with Notify.	API and manually provided statistics
DroneSec Research	The DroneSec team conducts penetration tests, vulnerability analysis, aerial threat simulations and forensics on a variety of DCU which results in zero-day intelligence of various systems. Whilst respecting the privacy of our clients, statistics and agreed information is shared with Notify.	Incidents Whitepapers Research Papers Vulnerabilities and Exploits Open-Source Intelligence
Deep, dark and surface web communication channels	Groups, message boards and forums dedicated to modding and bypassing common drones and counter-drone controls. DroneSec actively participate and contribute in these forums to better understand the threats and risks relevant to our clients.	Manual and automated analysis based on keywords and word-clouds.
Information Security Sources	A variety of public and private sources within the Information	Vulnerabilities and Exploits Incidents

	Security, threat intelligence and Open-Source Intelligence (OSINT) communities provide Notify with recent, actionable information.	Whitepapers Research Papers Sentiment and Chatter
Newsletters and Email Lists	A variety of commercial (paid) and public sources. Gated content is exchanged with Notify within a strict agreement basis. Good examples of public sources include the Center for Study of the Drone (Bard College).	News Incidents Studies and Reports
Law Enforcement	Notify collects information from public, private and Freedom of Information (FOI) portals from Law Enforcement and shares combined metrics back to agencies.	Events Incidents Statistics
Proprietary aggregation software - Search Engines - Social Media - Government Sources	The DroneSec Notify secret sauce. Our aggregators, dorks, scripts and macros receive, filter and analyse DCU-related data, filtering for relevant and actionable information.	News Events Incidents Whitepapers Research Papers Sentiment and Chatter
Subscribers & Individuals	Subscribers of dronesec.xyz, dronesec.com and individual contacts provide manual reports to the Notify service. Contact us to see how exchanging Threat Intelligence could provide additional support to your organisation.	Incidents Research Papers Sentiment and Chatter

B.2. LIMITATIONS

Intelligence gathering reflects a point-in-time notification and/or analysis in-scope objectives (DCU). Future changes to the artefacts and the availability of new information could introduce retraction of statements or alter the wording, ratings and analysis of artefacts outlined within this report.

While DroneSec conducts in-depth fact-checking and evidence-based analysis of the information, sources and events, we aggregate information that may not be proven to be factual. Wherever possible, we try to mark this as such. DroneSec pushes for quality over quantity – but understands the needs for a broad approach to intelligence within DCU. Not all Notify reports will include analysis; delivery is subject to time the Intelligence is detected and its availability at time of Notify release.

Another limitation to the report is the lack of introductory material for a new reader to the DCU space. While news events, situations and analysis can help, newcomers to the industry can get in touch with us at info@dronesec.com or via the slack channel to seek additional clarification on topics, phrases or informational courses that might uplift their knowledge and understanding in the area.