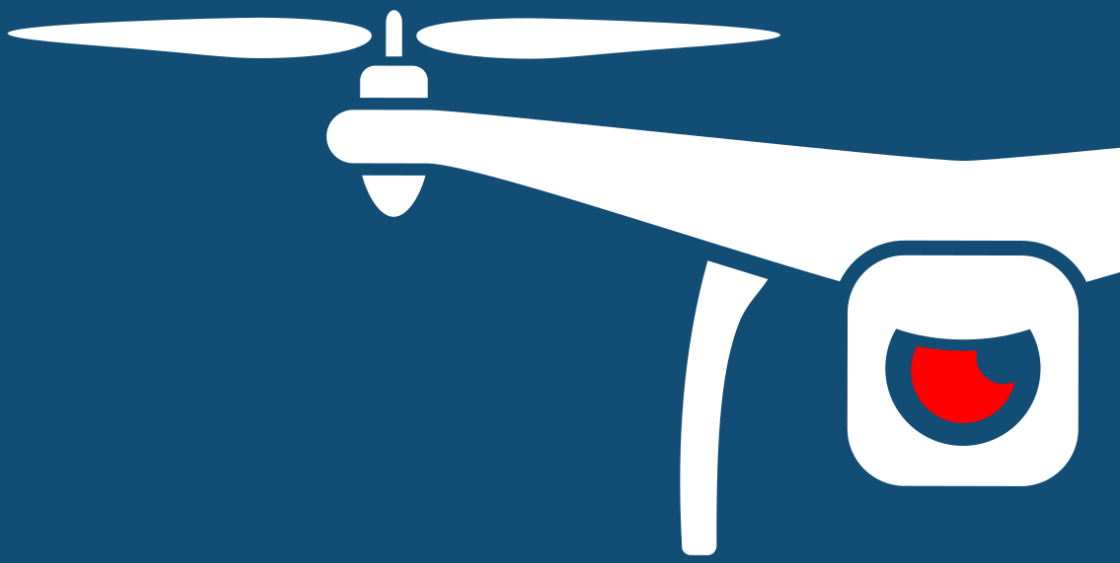
DRONE SEC
A Privasec COMPANY

NOTIFY ISSUE #24

WEEKLY THREAT INTELLIGENCE

27 May 2020 | 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

A dedicated 'cyber-security' section this week as a number of artefacts belong in that category. When threat modelling an actor who misuses drones, there are several characteristics. One is how technically savvy they may be at removing No-Fly-Zones (NFZs) and bypassing the mechanisms on drones themselves. For drone enthusiasts and modders – easily done. However, for the majority of contraband deliveries into prison, the apprehended subjects are often using pre-purchased and pre-made equipment, falling into the unskilled category.

To this extent, we track several NFZ bypass and pay-to-mod entities. If a drone or device is found by forensics to contain these binaries/applications/programs, it could link back to much needed information regarding the threat actor. This week, we see the return of the previously-thought-defunct "NoLimitDronez (NLD)" modding site that offers financial bounties in return for exploits leading to jailbreaks and other bypasses. Finally, a very interesting, yet brief analysis of the DJI Mimo app's undermining privacy and security features as investigated by River Loop Security.

Continuing in on the emerging technology side, a shift in the attitude of the Counter-Drone industry – with Citadel Defense releasing a counter-counter-drone software release against adversarial spoofing. This is where a threat actor might look to confuse or overwhelm a C-UAS system by mimicking drones or drone swarms that aren't really in the air. An example – a Raspberry Pi squawking drone MAC an BSSID addresses could do something similar on a trivial Wi-Fi scale. For Citadel's systems, it seems to come in the form of detecting and filtering out rogue Radio Frequency signals by using the "DeepFake" software. Will we see a whitepaper one day? Who knows, the tech is likely kept pretty watertight.

Notable events this week include the temporary halt of the Vance Air Force Base by drone, some great forensic analysis of piecing together a downed Altura Zenith drone and a halt on the European drone regulations by the aviation community on unaddressed privacy and safety concerns. Of personal interest, was footage streamed from a UK police drone showing a runaway suspect in action – no place to hide and quickly apprehended by a hovering law enforcement drone above.

I'd like to give a special thank you to Randall Nichols who heads up the UAS Cybersecurity practice at Kansas State University. First noticing Randall was providing insights at an upcoming webinar, he's kindly provided two of his drone security books to Notify readers, free of charge. In depth, highly relevant and taking on the core concepts of cyber security within unmanned systems, they're worth a read or storing on the Red Team's desk. Both of these eBooks can be found in the Whitepapers section.

- *Mike Monnik, DroneSec CTO*

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 few rounds in 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. If you missed the previous issue, please email us.

1.2. FEATURED ADVISORIES (P2)

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

Intrusion and Trespass	Priority
Illegal drone intrusion shuts down Vance Air Force Base for 2 hours	P2

Summary

A fighter pilot flew within 1,000ft of a drone during a training rehearsal and a call was made by the airbase to shut operations due to the infringement.

Overview

During a planned training rehearsal, one of the T-38 fighter pilots spotted a drone hovering at about 1,500ft and determined they were flying with approximately 1,000ft separation proximity to the drone. A call was made by the air base supervisor to shut the airbase and cease operations while the drone and its operator was searched for by the local police. However, neither was found. The drone was flying over a high school rather than the air base itself, however, that path was the flight path of manned airplanes into Vance Air Base.

The drone has infringed the height clearance of 400ft as well as its proximity in a restricted area nearby the airfield, both rules which were set by the FAA years prior.

Analysis

Threat Actor Intel: *Unknown*

Likelihood: *Uninformed / Infringing Hobbyist*

Rules on drone operation can be found online in the local government aviation websites and mobile applications for the convenience of operators. Despite multiple public broadcasts on what can and cannot be legally flown with drones, there are still many operators who continue to disregard these rules due to ignorance or plain disregard of aviation law. However, this instead has a negative effect on the innovation within the drone industry as regulators will enforce more stringent rules to clamp down on these errant operators – sometimes, affecting the legitimate and commercial drone operators more than the intended party.

Drone laws are set in place for safety reasons. A study from the FAA also concluded that drone strikes caused more damage to aircrafts and helicopters than bird strikes, due to the hard and rigid components of drones. With the capabilities of drones being able to fly further and higher, these advancements are beneficial when utilised correctly, but cause harm when not adhering to regulations set in place by authorities.

Recommendation

Remote Identification and UAS Traffic Management (UTM) systems are a proactive approach to managing incidents between drones and manned aircraft. UTM systems enforce safe coexistence of unmanned and manned aircrafts, reducing the risk of safety infringements and potential loss of life. Drone operators should be cognisant with the laws of their country and have the appropriate licenses if required. Operators should aim to keep themselves up to date or relevantly trained before operating a drone.

In areas where counter-drone or drone detection systems are not readily available, undertaking table-top simulations or exercises to counter for scenarios like these are essential. Training is recommended for non-operators working in a field that could be affected (both directly and indirectly) by rogue or disruptive drones. Furthermore, organisations should have a Standard Operating Procedure (SOP) or Incident Response Plan in play to mitigate potential delays, overcome landing preventions and quickly involve the appropriate law enforcement bodies.

References:

https://www.enidnews.com/news/local_news/updated-police-respond-to-report-of-drone-illegally-entering-vance-airspace/article_995404c6-c7fa-544b-9522-d07f9496c703.html

Safety	Priority
Downed Aerialtronics Altura Zenith ATX8 cause due to magnetic interference over railway tracks	P2

Summary

A drone, shortly after takeoff, drifted and accelerated away from the operator, crashing into vegetation without active control or regain of control.

Overview

An Aerialtronics Altura Zenith ATX8, utilised for aerial work at the railway tracks, took off in GPS mode and climbed to an altitude of 5m before it started to drift to the west. As the drone continued ascending to about 10m, it suddenly accelerated to the west and began to lose altitude. The drone operator attempted to correct the drift but was unable to establish control of the drone before it flew away out of sight and into vegetation next to railway tracks in Gloucestershire.

Analysis

The manufacturer analysed the flight log data and verified that the magnetic compass of the drone has a variance of 60 degrees shortly after takeoff. Even though the operator's input were detected by the drone, the drone continued to move in a westerly direction and descended over a distance of 100m before crashing.

Investigation has also shown that while radio frequencies at the takeoff site was not disrupted, magnetic compass readings at the site were off the charts., with a deviation of 140 degrees. The deviation was present in areas where the overhead railway track's high-voltage wires were being ducted.

With this finding, several operational procedures had to be altered such as the change in takeoff position away from sources of magnetic interference and the need to operate the drone in manual mode (instead of GPS mode) in events of emergencies such as this.

Recommendation

It is recommended that drone operators have a good understanding on the capabilities of their drones –the intricate command functions available in the drone in every possible scenario, flight time, range and protocols or frequencies in use. Practice of the worst-case scenario (Red Team and War Room scenarios) happening and work backwards to ensure you and your team have appropriate controls. These are important details which aid operators in planning their pre-flight mission and handling ad-hoc changes when unexpected contingencies may occur mid-flight.

In the event something like this occurs, the crew should also have a forensic or incident response kit ready and waiting to collect the evidence, hardware and software data to piece together the story of what happened. Logging on both the drone, controllers and interconnected systems/software should provide enough telemetry data to discern what is accidental link-failure, bird strike or operator mistake over a malicious de-authentication attack, signal jam or protocol manipulation of the devices.

It is always recommended to select a (drone and control link) brand that has been independently tested from a security and penetration testing point of view, conduct a simulation catering for malicious individuals targeting the event for mitigation and remediation purposes. This is something DroneSec provides as a core speciality – please contact info@dronesec.com to enquire about Red Teaming and Aerial Threat Simulation services.

References

https://www.theregister.co.uk/2020/05/21/drone_electromagnetic_interference/

https://assets.publishing.service.gov.uk/media/5e96dfdae90e071a18ca10ae/Aerialtronics_Altura_Zenith_ATX8_na_011019_05-20.pdf (PDF Document)

Security	Priority
Drone drug-delivery attempt at Mansfield Correctional Institution results in arrest.	P2

Summary

A man was arrested for possessing a drone and packages containing narcotics and cell phones near a prison.

Overview

A call was made after a drone was spotted flying in the vicinity of Mansfield prison. Officers rushed to the approximated area and found a man in a vehicle also containing a drone and packages of contraband. However, there was a second drone in the air and the man was arrested was not flying said drone. Investigation are still ongoing into the operator of the second drone.

Analysis

Tracked Actor Category:

Prison Drone Delivery (Local Disruptors)

Motivation and Goals:

- Use of unmanned systems to supply incarcerated individuals;
- Use of unmanned systems to separate the distance and risk between operators and contraband payloads;
- Use of unmanned systems to conduct reconnaissance and delivery missions;
- Use of unmanned systems to overcome physical and personnel security barriers and controls;

Tactics, techniques and procedures:

- Sourcing cheap and available Commercial-Off-The-Shelf (COTS) drones for one-way flights;
- Bypassing No-Fly-Zones (NFZ) and restricted airspace by modding;
- Self-taught in unmanned and contraband-delivery UAS flights and operations;
- Using small COTS drones to drop contraband (cellphones, narcotics, weapons ~<2kgs) onto prison grounds, often with purchased or home-made dropping mechanisms;
- In rare cases, utilising counter-forensics techniques by removing SD cards, disabling caching, destroying serial info and disabling the Return-to-Home functionality;

Recorded use of drone and equipment types:

- Quadcopters, Multi-rotors
- PGYTECH Air Dropping System

References

https://www.mansfieldnewsjournal.com/story/news/2020/05/26/patrol-averts-drone-contraband-drop-over-manci/5258000002/

Exploits and Vulnerabilities	Priority
River Loop Security reveals privacy concerns over DJI Mimo app	P2

Summary

River Loop Security firm reviewed the DJI Mimo app's binaries and network traffic, discovering some items which they believe are concerning for US citizens, companies and policy makers.

Overview

River Loop Security has summarised the key findings of performing security analysis on the application as

follows, The DJI Mimo app:

- Uses libraries that request personal data about users' religious and political affiliation, as well as security settings from connected social network APIs.
- Sends data through insecure means to servers behind the Great Firewall of China, where it is accessible to the Chinese Government.
- Requests from users (via the OS) access to fine and coarse location data, the ability to manipulate Wi-Fi state, read SMS messages, and read logs.
- Fails to meet basic security practices for users' data, leading to potential disclosure or modification in transit.
- DJI's Terms of Use Agreement allows user data to be shared with the Chinese Government.
- Even without user consent, the DJI Mimo app sends sensitive information via unsecured means to third-party servers, where the Terms of Use Agreement supports cooperation with the Chinese Government.

Analysis

DJI Mimo is just one of the many mobile applications provided by DJI for its drone products. From our analysis of the article, the root causes can be attributed to:

- The intrusive and social-based data-points are quite standard for the listed analytics services, however, can extract and utilise that information for malicious use.
- Overly permissive mobile device permissions – some of these may be for genuine use cases but does not prevent them from being misused.
- Weak transport and communication security means attackers intercepting the data could do so with ease.
- Overly restrictive terms and conditions potentially preventing appropriate legal recourse.

The authors produce a number of future research points which can be examined and contrast their findings to that of the previous Kivu Consulting commissioned engagement by DJI.

References

https://www.riverloopsecurity.com/blog/2020/05/dji_mimo/ (Main Article)

https://gizmodo.com/dji-releases-security-findings-it-hopes-will-quash-chin-1825469976?IR=T

https://www.dji.com/newsroom/news/independent-study-validates-dji-data-security-practices

https://www.dropbox.com/s/u221xdd3w0tkde6/Kivu%20summary%20of%20DJI%20report.pdf?dl=0

1.3. CYBER SECURITY (P3)

Analysing data use by the DJI MIMO application

https://www.riverloopsecurity.com/blog/2020/05/dji_mimo/

Drone bounty site for No-Fly-Zone exploits, jailbreaks and bypasses sees return and updates

https://nolimitdronez.com/

Apple device application modding site emerges for drone No-Fly-Zone exploits and bypasses

http://www.hackgoapp.com/

Drone Penetration Testing and Vulnerability Analysis Framework to be released at RSA Conference 2020

https://www.rsaconference.com/apj/apj-2020/agenda/drone-penetration-testing-and-vulnerability-analysis-framework

Attacking and Defending against Drones – PHACK 2020

https://www.youtube.com/watch?v=CcFnJ9DLVsQ

https://github.com/rsfl/researchdocs/blob/master/RSoto_Attacking_Defending_Against_Drones_FINAL_2020_Links.pdf (PDF Download)

1.4. NEWS AND EVENTS (P3)

Vinveli supplies Vero drones armed with grenade launcher to India

https://www.forbes.com/sites/kelseyatherton/2020/05/18/farming-drone-goes-from-plowshares-to-grenade-launcher/#5d7c1d18b572

Artsakh military trial tests suicide drone for military usage

https://armenpress.am/eng/news/1015819.html

Drugs and drones and how to stop them (Commentary)

https://www.airspacemag.com/flight-today/narcodrones-180974934/

Dental clinic reported to police for drone use by public, Wombourne, UK

https://coronavirus.dental-tribune.com/news/dentist-reported-to-police-for-using-drone-to-take-care-of-patient/

1.5. WHITEPAPERS, PUBLICATIONS & REGULATIONS (P3)

New Minnesota law on search warrants and privacy for Law Enforcement using drones

https://www.lmc.org/news-publications/news/all/drones-bills-update/

FAA opens survey for developing national forecasts of UAS activity, closing July 14, 2020

https://www.federalregister.gov/documents/2020/05/12/2020-10139/agency-information-collection-activities-requests-for-comments-clearance-of-a-new-approval-of

European aviation community requests for halt in drone regulation for more discussion on unaddressed concerns

https://www.ainonline.com/aviation-news/business-aviation/2020-05-19/european-orgs-ask-more-industry-input-drone-regs

The use of UAVs within Conflict Monitoring Missions

https://muse.jhu.edu/article/754943 (PDF Download)

Evaluating LAANC Utilisation & Compliance for sUAS in Controlled Airspace

https://commons.erau.edu/ijaaa/vol7/iss2/4/ (PDF Download)

Counter Unmanned Aircraft Systems Technologies and Operations

https://newprairiepress.org/ebooks/31/ (PDF Download)

Unmanned Aircraft Systems in Cyber Domain: Protecting USA's Advanced Air Assets (2nd edition)

https://newprairiepress.org/ebooks/27/ (PDF Download)

PARTH: A two-stage lightweight mutual authentication protocol for UAV surveillance networks

https://www.sciencedirect.com/science/article/abs/pii/S0140366419318456 (PDF available for Notify customers)

1.6. COUNTER DRONE SYSTEMS (P3)

Citadel Defence adds deepfake capabilities to Titan C-UAS system against spoofing tactics

https://www.businesswire.com/news/home/20200526005057/en/Citadel-Defense-Launches-Deepfake-AI-Prevent-Drone

US Navy conducts test of high-powered anti-drone laser system onboard USS Portland

https://news.usni.org/2020/05/22/video-uss-portland-fires-laser-weapon-downs-drone-in-first-at-sea-test

https://twitter.com/USPacificFleet/status/1263932322048434176

DroneShield launches DroneOptID, an optical drone detection, identification and tracking tool

https://www.droneshield.com/press-releases-content/2020/5/25/droneoptid-launch

European Union police awards DroneShield on supply and training of DroneGun Tactical

https://www.droneshield.com/press-releases-content/2020/5/21/droneshield-chosen-by-the-european-union-police

1.7. UTM SYSTEMS (P4)

Leidos awarded contract to upgrade US Army Unmanned Ground Control Station

https://www.leidos.com/insights/leidos-awarded-contract-advance-us-armys-unmanned-aircraft-ground-control-system

1.8. DRONE TECHNOLOGY (P5)

World of Drones and Robotics Congress opens abstracts for 2020 conference in Australia

https://www.defensenews.com/air/2020/05/20/more-than-one-company-could-get-cash-to-build-the-air-forces-ai-equipped-skyborg-drone/

Chinese developed helicopter-drone, AR500C, to be deployed at China-India border

https://www.hindustantimes.com/india-news/new-chopper-drone-may-be-deployed-along-india-border-chinese-state-media/story-DQUUa0f1flgrPQYDo06oII.html

Drones used to monitor volcanic activities, reduce risk to volcanologists

https://www.sciencedaily.com/releases/2020/05/200525115649.htm

US Army develops ultra-thin wideband metaferrites antenna for possible SATCOM with drones

https://www.army.mil/article/235700/army_mantech_program_advances_materials_for_new_low_profile_antenna

MQ-8C and MQ-60 unmanned naval helicopters to possibly have armed torpedos for US Navy

https://news.northropgrumman.com/news/features/northrop-grumman-builds-very-lightweight-torpedo-for-us-navy

US Air Force starts competition for Skyborg AI-based drone that makes decisions in battle

https://www.defensenews.com/air/2020/05/20/more-than-one-company-could-get-cash-to-build-the-air-forces-ai-equipped-skyborg-drone/

1.9. INFORMATIONAL (P5)

Drone leads to arrest of two individuals after high speed pursuit in Johnson County, USA

https://www.paintsvilleherald.com/news/police-use-k9-drone-in-high-speed-pursuit-couple-arrested/article_67c19ef8-9a6d-11ea-bff9-cf41586da228.html

Police drone footage shows suspect hopping over fences and gardens to escape arrest, UK

https://www.bbc.com/news/av/uk-england-nottinghamshire-52740908/police-drone-footage-shows-garden-hopping-suspect

Vehicle thief caught in Rice County with the help of drones, Minnesota, USA

https://www.southernminn.com/faribault_daily_news/news/article_e71c0099-de69-534d-bccd-86d25cd31891.html

Colombian police use thermal drones to detect body temperatures amidst COVID19

https://www.physiciansweekly.com/colombian-police-use-drones/

Greece to reopen beaches but will utilise drones to monitor social distancing

https://www.lonelyplanet.com/articles/greece-beach-drones-social-distancing

Howard County PD uses drone in search, Baltimore, Maryland, USA

https://foxbaltimore.com/news/local/missing-barefoot-14-year-old-walked-away-from-home-k-9-drone-search-unsuccessful

Matrice 200 drone used by Scotland PD in search for mission person, Aberdeen, UK

https://www.pressandjournal.co.uk/fp/news/aberdeen/2212793/police-use-drones-in-search-for-missing-74-year-old-aberdeen-man/

Missing elderly in Orange, California, found with drone, USA

https://www.ocregister.com/2020/05/25/police-use-drone-to-find-a-missing-woman-in-orange/

https://twitter.com/CityOfOrangePD/status/1265069054877786112

South Korea Coast Guards demonstrates drones to catch abalone thieves and in Wando County

http://www.ajudaily.com/view/20200522123505160

Drone used in 5-hour rescue to pinpoint hiker fallen from cliff, Utah, USA

https://gephardtdaily.com/local/utah-man-hoisted-from-cliff-flown-to-hospital-after-fall-near-jones-hole/

Bullock County EMA receives Matrice 200 drone for law enforcement, Alabama, USA

http://www.unionspringsherald.com/news/article_82f04030-9adb-11ea-a83a-a367a78a82b5.html

NT Police, Fire and Emergency Services request tender for 4 DJI Matrice 300 RTK drones

https://tendersonline.nt.gov.au/Tender/ClosedDetails/9165

1.10. SOCIALS (P5)

Israeli army UAV activity over Tyre and Nabatieh in Lebanon

https://twitter.com/no_itsmyturn/status/1264939706715975681

Surveillance drones spotted over the Gaza strip

https://twitter.com/IsraelGazaICN/status/1264652800987811840

Pearland Police Department drone program

https://www.youtube.com/watch?v=FpkEsmU1NEo

Satellite images show GNA build airstrip in Tripoli city for Turkish-Made Bayraktar TB2 drones

https://twitter.com/mahmouedgamal44/status/1263708813951209472

Epsilon 175 Fixed Wing UAV demonstrates covert tracking of enemy troops

https://www.youtube.com/watch?v=-ef-C506Hzs

Spying on America by Foreign-made Drones (Webinar @1)

https://youtu.be/xXX7ClnfBfU (Part A)

https://youtu.be/cGqOXafpT7M (Part B)

Spying on America by Foreign-made Drones – Cyber Security Elements and Risks (Webinar #2)

https://www.bigmarker.com/usa-drone-port/Spying-on-America-by-Foreign-made-Drones-Part-2

Use of Drones in Public Order Policing – Drone Con (Webinar)

https://www.youtube.com/watch?v=kW4oF2lZvO0

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.

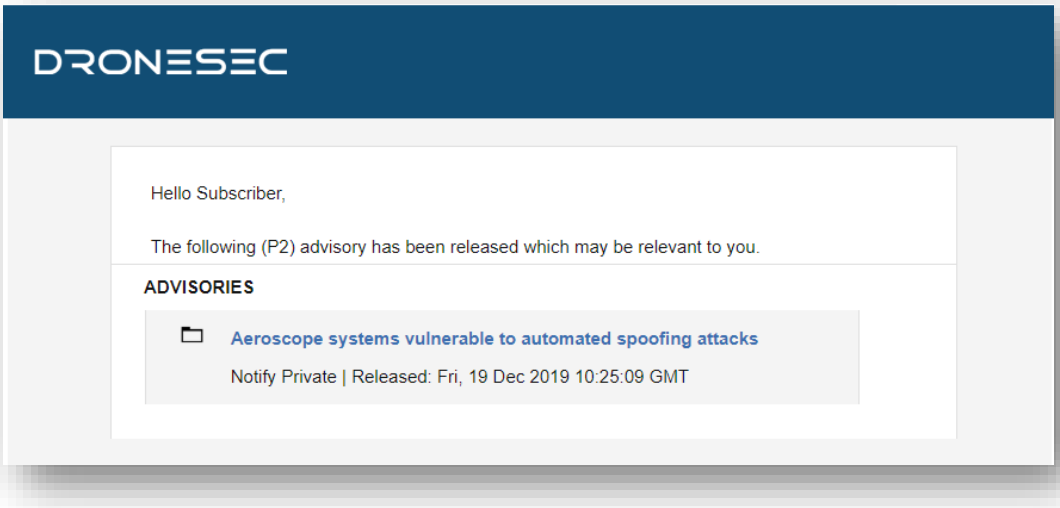


Figure 1 - A threat notification specific to a Notify customer's listed keywords.

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[1], UAV[2], RPAS[3]… • 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

[1] UAS: Unmanned Aerial System
[2] UAV: Unmanned Aerial Vehicle
[3] RPAS: Remotely Piloted Aerial System

	• Detect and/or respond to drones • Be standalone, hand-held, static or integrated with a UTM[4] or PSIM[5] 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[6], exploits or zero-days[7]. 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

[4] UTM – Universal Traffic Management System
[5] PSIM – Physical Security Information Management System
[6] OSINT: Open-Source Intelligence from the public domain.
[7] 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.