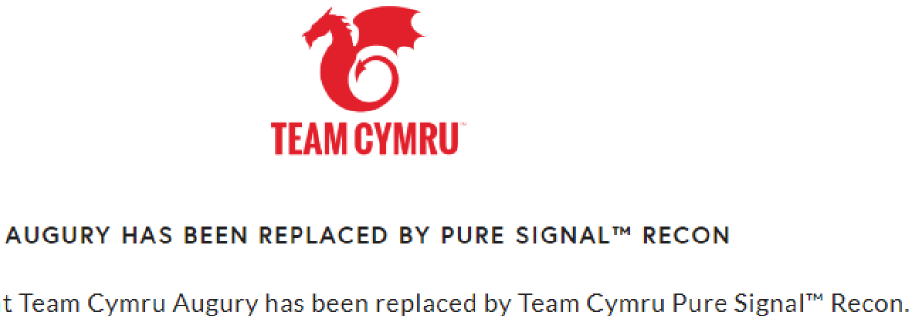
As the word means, "Pure Signal", in its simplest terms, aims to transmit without interference and to transmit the interference data after it has been made simple and analysable. Whether you use PowerSDR products, listen to standard radio transmissions, or analyze traffic flowing through the network, you want the data to be as clear as possible.

Developed by Team-Cymru, "**Pure Signal Recon**", formerly **AUGURY**, seems to have taken its basic philosophy from the above brief description.



AUGURY HAS BEEN REPLACED BY PURE SIGNAL™ RECON

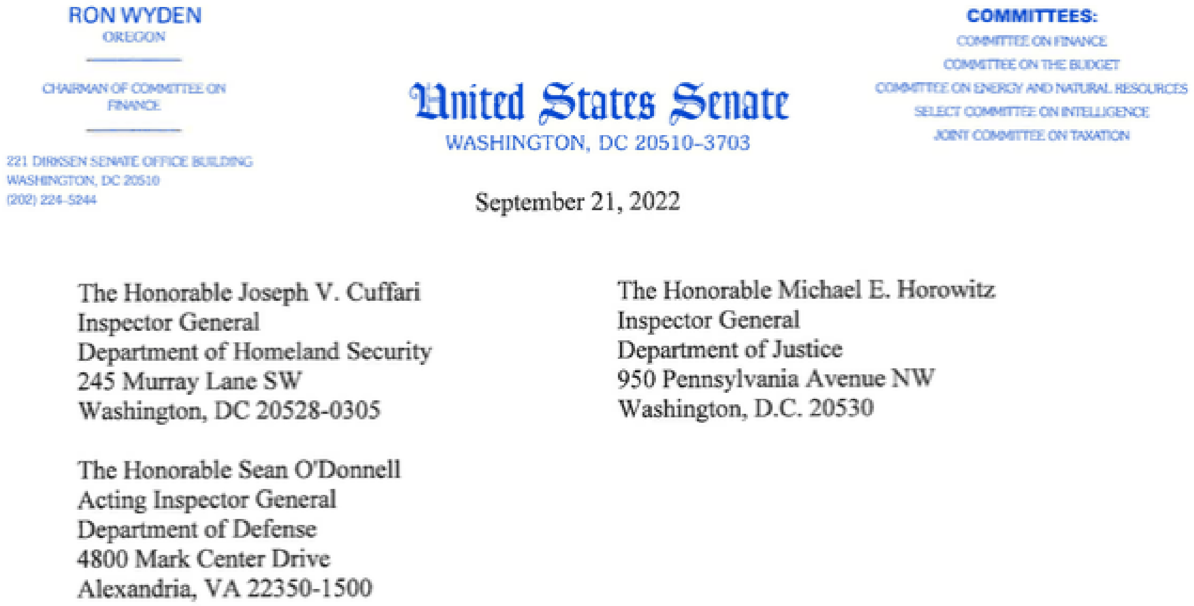
Please note that Team Cymru Augury has been replaced by Team Cymru Pure Signal™ Recon.

It is believed that one of the law enforcement agencies affiliated with the US military, some of which are within the Navy, NCIS (**Naval Criminal Investigative Service**), purchased and used this product. Today, NCIS operates in approximately 191 locations, in more than 41 countries. NCIS has used data streams many times in the past years.

This became known when an anonymous whistleblower contacted Senator Ron Wyden. Whistleblower said that with this "tool", which was sold to military institutions, almost all internet activities, browser traces and network traffic of American citizens can be accessed without permission. Within this scope, it has also revealed the sale of data warehouses from some unnamed institutions that host the users' data to more than one American official institution. One of these official institutions is the Defense Intelligence Agency. The Senator also noted that several times the DoD-Pentagon (United States Department of Defense) has blocked efforts to investigate and clarify the government's purchase of internet browsing records of users.

CUI (**Controlled Unclassified Information**) acts as a shield against leaking information for institutions such as DoD.

Although there are blockings and information masking, under the CUI (**Controlled Unclassified Information**) restrictions, the senator also stated that he managed to get answers to some of his parliamentary questions thanks to open sources such as public contract information. According to some of these published online-public contract files, it has been revealed that many institutions affiliated to DoD, data belonging to citizens have been purchased many times from data mining companies.The most striking examples are: The Defense Counterintelligence and Security Agency spent more than $2 million purchasing access to netflow data, and the Defense Intelligence Agency purchased Domain Name System data.



RON WYDEN
OREGON

CHAIRMAN OF COMMITTEE ON
FINANCE

221 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-5244

United States Senate
WASHINGTON, DC 20510-3703

COMMITTEES:
COMMITTEE ON FINANCE
COMMITTEE ON THE BUDGET
COMMITTEE ON ENERGY AND NATURAL RESOURCES
SELECT COMMITTEE ON INTELLIGENCE
JOINT COMMITTEE ON TAXATION

September 21, 2022

The Honorable Joseph V. Cuffari
Inspector General
Department of Homeland Security
245 Murray Lane SW
Washington, DC 20528-0305

The Honorable Michael E. Horowitz
Inspector General
Department of Justice
950 Pennsylvania Avenue NW
Washington, D.C. 20530

The Honorable Sean O'Donnell
Acting Inspector General
Department of Defense
4800 Mark Center Drive
Alexandria, VA 22350-1500

The Senator also underlined that although he applied for the reassignment of information to the DoD with these documents, he was again rejected. Considering this dominant situation of the internet structure and the money addiction of the free-market economy, it is inevitable to experience such situations.

Meanwhile, the importance of the whistleblower takes the stage. The aforementioned whistleblower has previously objected to data sales to many institutions. This whistleblower stated that NCIS has repeatedly purchased network streams, including communication log data, from data broker Team Cymru. In the signed contracts, the product name "Augury" is mentioned. Its current name is "Pure Signal" and it has many variations such as Pure Signal Orbit.

Based on evidence based on public procurement records, it has been learned that this product acquires and stacks petabytes of data and has the capacity to record close to 100 billion pieces of data per day. This tool uses a common database with many third party companies.

In addition, the product ensures that the route map of the end-point providing a data flow can also be drawn by mapping the proxies and VPNs. Access to mail protocols data (IMAP/POP/SMTP) in application layers can also be provided. Pure Signal can also monitor open port maps, network flows, PDNs, X.509 certificates and many other network signatures. With the ant route disclosure logic, it can clearly reveal network maps of an IP providing the traffic and other endpoints connected to that IP.

Below is a list of data obtained by this intercontinental tool:

- **DNS history (forward and reverse)**
- **Operating system fingerprinting**
- **IRC keyword analysis**
- **NMAP scans**
- **Pastebin archived data**
- **Banners on networked devices**
- **Beaconing activity**
- **Cookie usage**
- **UserAgent data**
- **Extracted file information**
- **IMAP/POP/SMTP**
- **RDP/FTP**
- **URLs accessed**
- **x509 Certs**

It appears that the first sample commercial submission is related to this address **coleen.johnson@navy.mil** (Coleen Johnson 2156973388). Product Service Code is also **7A21** - IT AND TELECOM - BUSINESS APPLICATION SOFTWARE. This also indicates a high-level purchase authorization.

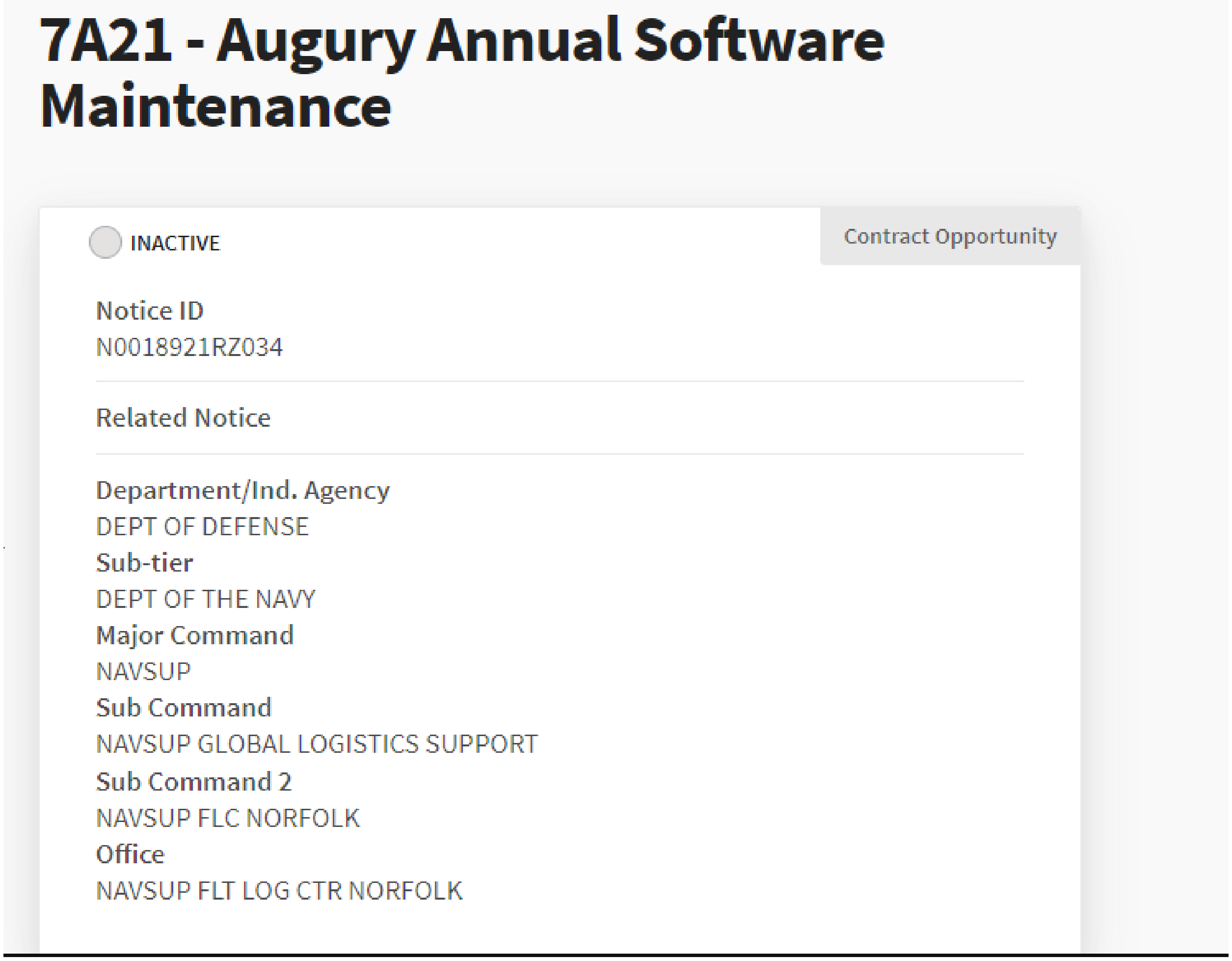
It is useful to note the following fact about the aforementioned X.509 certificates:
The most common use case of X.509-based PKI is Transport Layer Security (TLS)/Secure Socket Layer (SSL), which is the basis of the HTTPS protocol, which enables secure web browsing. This is a globally accepted International Telecommunications Union standard. It is at the core of many networks infrastructure security, P2P secure communication, and encrypted communication of application layer protocols. The X.509 certificate is a safeguard against malicious network impersonators.The majority uses SHA256.

The product marketing catalog reads:
"*Our Commercial tool Pure Signal™ RECON (known by our legacy clients and partners as Augury) has, as one of its 50+ data types, x.509 certificates as a search option.*"

Team Cymru has declared that it has millions of data on these certificates. It stated in one of its advertisements that they examine between 2 million and 8 million pieces of data on average every day. They do this with the certificate information they collect from everywhere in this data store. This multiple data acquisition situation is possible through relationships with many private institutions and organizations and many layers of ISPs.

It is underlined that this tool also records data from approximately 550 points spread around the world. According to the official registration number **N0018921RZ034**, these data collection centers are spread over many continents. The network data includes collection points in Europe, the Middle East, North/South America, Africa and Asia.

There are two separate applications, September and January 2021:



7A21 - Augury Annual Software Maintenance

○ INACTIVE

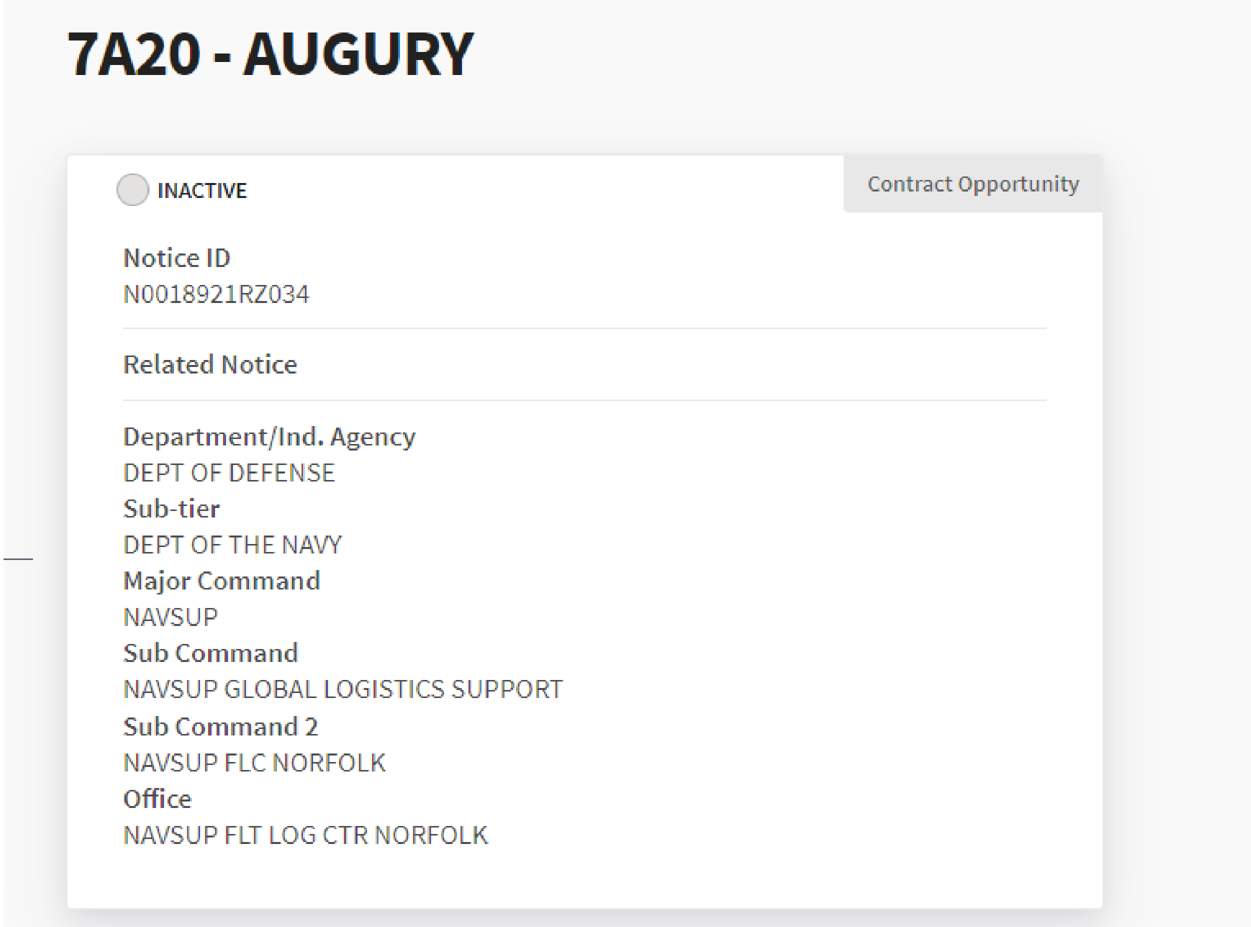
Contract Opportunity

Notice ID
N0018921RZ034

Related Notice

Department/Ind. Agency
DEPT OF DEFENSE
Sub-tier
DEPT OF THE NAVY
Major Command
NAVSUP
Sub Command
NAVSUP GLOBAL LOGISTICS SUPPORT
Sub Command 2
NAVSUP FLC NORFOLK
Office
NAVSUP FLT LOG CTR NORFOLK

- https://sam.gov/opp/81b3e986cef44c0cb805f121b0761353/view?keywords=&sort=-modifiedDate&index=opp&is_active=true&page=34



7A20 - AUGURY

○ INACTIVE

Contract Opportunity

Notice ID
N0018921RZ034

Related Notice

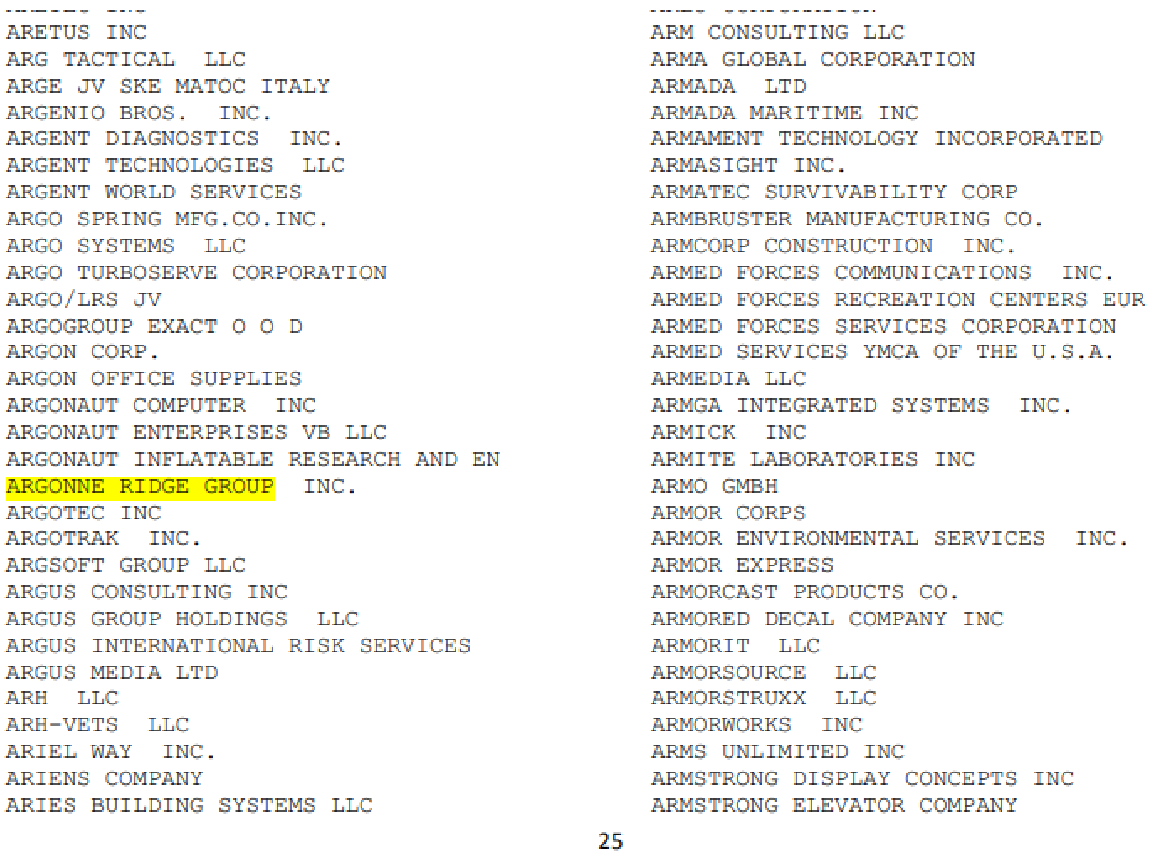
Department/Ind. Agency
DEPT OF DEFENSE
Sub-tier
DEPT OF THE NAVY
Major Command
NAVSUP
Sub Command
NAVSUP GLOBAL LOGISTICS SUPPORT
Sub Command 2
NAVSUP FLC NORFOLK
Office
NAVSUP FLT LOG CTR NORFOLK

- https://sam.gov/opp/96b4874e76af45be90bb5a0b8b2bdb6b/view?keywords=&sort=-modifiedDate&index=opp&is_active=true&page=28

The product is indeed very similar to Palantir's Gotham Project.

Within the scope of this research, it was also revealed that the government contractor, Argonne Ridge Group, is actually a mirror of Team Cymru and have the same corporate address and employee profiles. This institution, known for its closeness to governments, has contracts with the U.S. Cyber Command, the Army, the Federal Bureau of Investigation and the U.S. Secret Service. Most of the agreements use this company title. It has also been confirmed by open-public contracting that the meta-records(metadata) of the Internet have been sold to many US-based military and civilian intelligence agencies many times under the cover of Argonne Ridge Group.

Argonne Ridge Group has received more than $25 billion in grants, according to a report that was published by DOD, 2015.

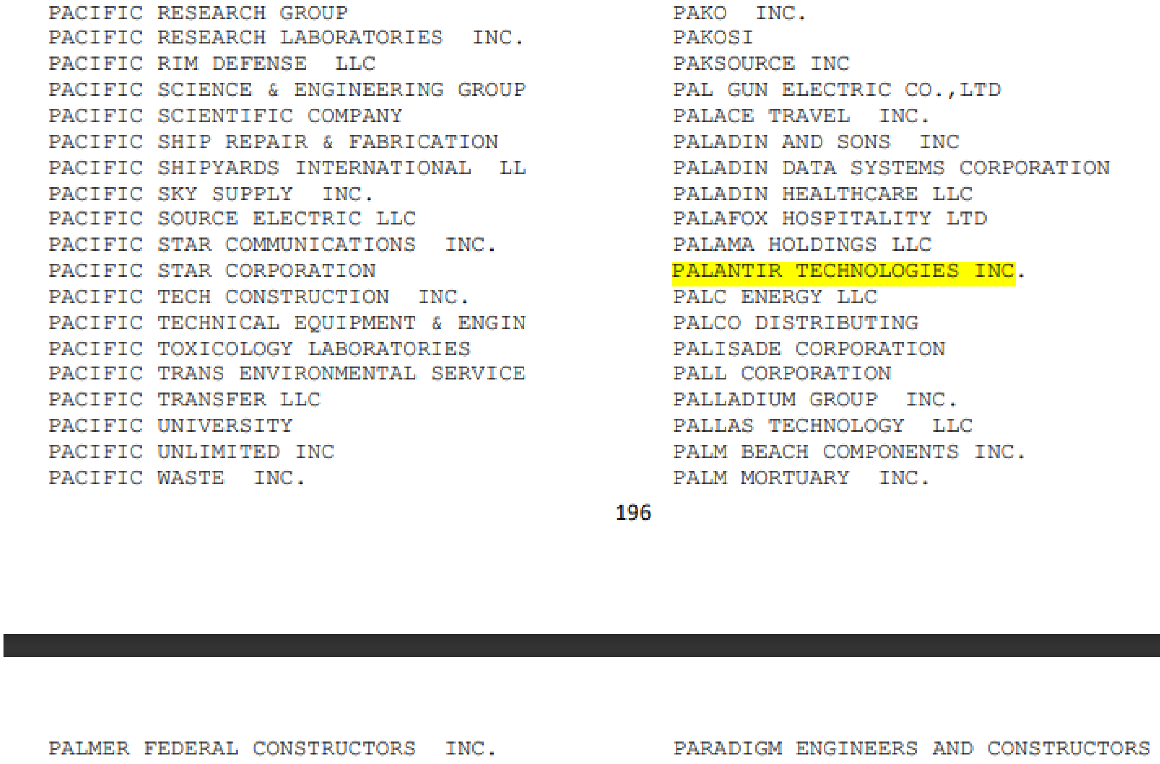


```
ARETUS INC
ARG TACTICAL  LLC
ARGE JV SKE MATOC ITALY
ARGENIO BROS.  INC.
ARGENT DIAGNOSTICS  INC.
ARGENT TECHNOLOGIES  LLC
ARGENT WORLD SERVICES
ARGO SPRING MFG.CO.INC.
ARGO SYSTEMS  LLC
ARGO TURBOSERVE CORPORATION
ARGO/LRS JV
ARGOGROUP EXACT O O D
ARGON CORP.
ARGON OFFICE SUPPLIES
ARGONAUT COMPUTER  INC
ARGONAUT ENTERPRISES VB LLC
ARGONAUT INFLATABLE RESEARCH AND EN
ARGONNE RIDGE GROUP  INC.
ARGOTEC INC
ARGOTRAK  INC.
ARGSOFT GROUP LLC
ARGUS CONSULTING INC
ARGUS GROUP HOLDINGS  LLC
ARGUS INTERNATIONAL RISK SERVICES
ARGUS MEDIA LTD
ARH  LLC
ARH-VETS  LLC
ARIEL WAY  INC.
ARIENS COMPANY
ARIES BUILDING SYSTEMS LLC
```

```
ARM CONSULTING LLC
ARMA GLOBAL CORPORATION
ARMADA  LTD
ARMADA MARITIME INC
ARMAMENT TECHNOLOGY INCORPORATED
ARMASIGHT INC.
ARMATEC SURVIVABILITY CORP
ARMBRUSTER MANUFACTURING CO.
ARMCORP CONSTRUCTION  INC.
ARMED FORCES COMMUNICATIONS  INC.
ARMED FORCES RECREATION CENTERS EUR
ARMED FORCES SERVICES CORPORATION
ARMED SERVICES YMCA OF THE U.S.A.
ARMEDIA LLC
ARMGA INTEGRATED SYSTEMS  INC.
ARMICK  INC
ARMITE LABORATORIES INC
ARMO GMBH
ARMOR CORPS
ARMOR ENVIRONMENTAL SERVICES  INC.
ARMOR EXPRESS
ARMORCAST PRODUCTS CO.
ARMORED DECAL COMPANY INC
ARMORIT  LLC
ARMORSOURCE  LLC
ARMORSTRUXX  LLC
ARMORWORKS  INC
ARMS UNLIMITED INC
ARMSTRONG DISPLAY CONCEPTS INC
ARMSTRONG ELEVATOR COMPANY
```

25

PALANTIR TECHNOLOGIES INC was also on the same list.



PACIFIC RESEARCH GROUP
PACIFIC RESEARCH LABORATORIES INC.
PACIFIC RIM DEFENSE LLC
PACIFIC SCIENCE & ENGINEERING GROUP
PACIFIC SCIENTIFIC COMPANY
PACIFIC SHIP REPAIR & FABRICATION
PACIFIC SHIPYARDS INTERNATIONAL LL
PACIFIC SKY SUPPLY INC.
PACIFIC SOURCE ELECTRIC LLC
PACIFIC STAR COMMUNICATIONS INC.
PACIFIC STAR CORPORATION
PACIFIC TECH CONSTRUCTION INC.
PACIFIC TECHNICAL EQUIPMENT & ENGIN
PACIFIC TOXICOLOGY LABORATORIES
PACIFIC TRANS ENVIRONMENTAL SERVICE
PACIFIC TRANSFER LLC
PACIFIC UNIVERSITY
PACIFIC UNLIMITED INC
PACIFIC WASTE INC.

PAKO INC.
PAKOSI
PAKSOURCE INC
PAL GUN ELECTRIC CO.,LTD
PALACE TRAVEL INC.
PALADIN AND SONS INC
PALADIN DATA SYSTEMS CORPORATION
PALADIN HEALTHCARE LLC
PALAFOX HOSPITALITY LTD
PALAMA HOLDINGS LLC
PALANTIR TECHNOLOGIES INC.
PALC ENERGY LLC
PALCO DISTRIBUTING
PALISADE CORPORATION
PALL CORPORATION
PALLADIUM GROUP INC.
PALLAS TECHNOLOGY LLC
PALM BEACH COMPONENTS INC.
PALM MORTUARY INC.

196

PALMER FEDERAL CONSTRUCTORS INC.

PARADIGM ENGINEERS AND CONSTRUCTORS

Team Cymru's partner in Finland is a company called Arctic Security. Collaboration with this company has been carried out in many investigations of malicious internet activity that took place during the pandemic. Pure Signal was used in Europe for these network analyzes.

Team Cymru collaborates with the European Commission:
https://www.enisa.europa.eu/topics/csirts-in-europe/files/team-cumru/

One of the tragic-comic facts is that some of Team Cymru's former employees worked within the TOR Project.Also, CEO of Team Cymru, Rabbi Rob Thomas also sits on the board. He has also taken important roles in technology companies such as Cisco and AT&T Teleholdings and was the CEO of WW2 Armor. The education period also attracts a lot of attention.

2012 - **Jewish Spiritual Leaders Institute** (Religious Studies)
1989 - **US Navy/US Marine Corps Field Medical Service School** (Combat Medical Technician)
1988 - **US Navy Naval Hospital Corps School**

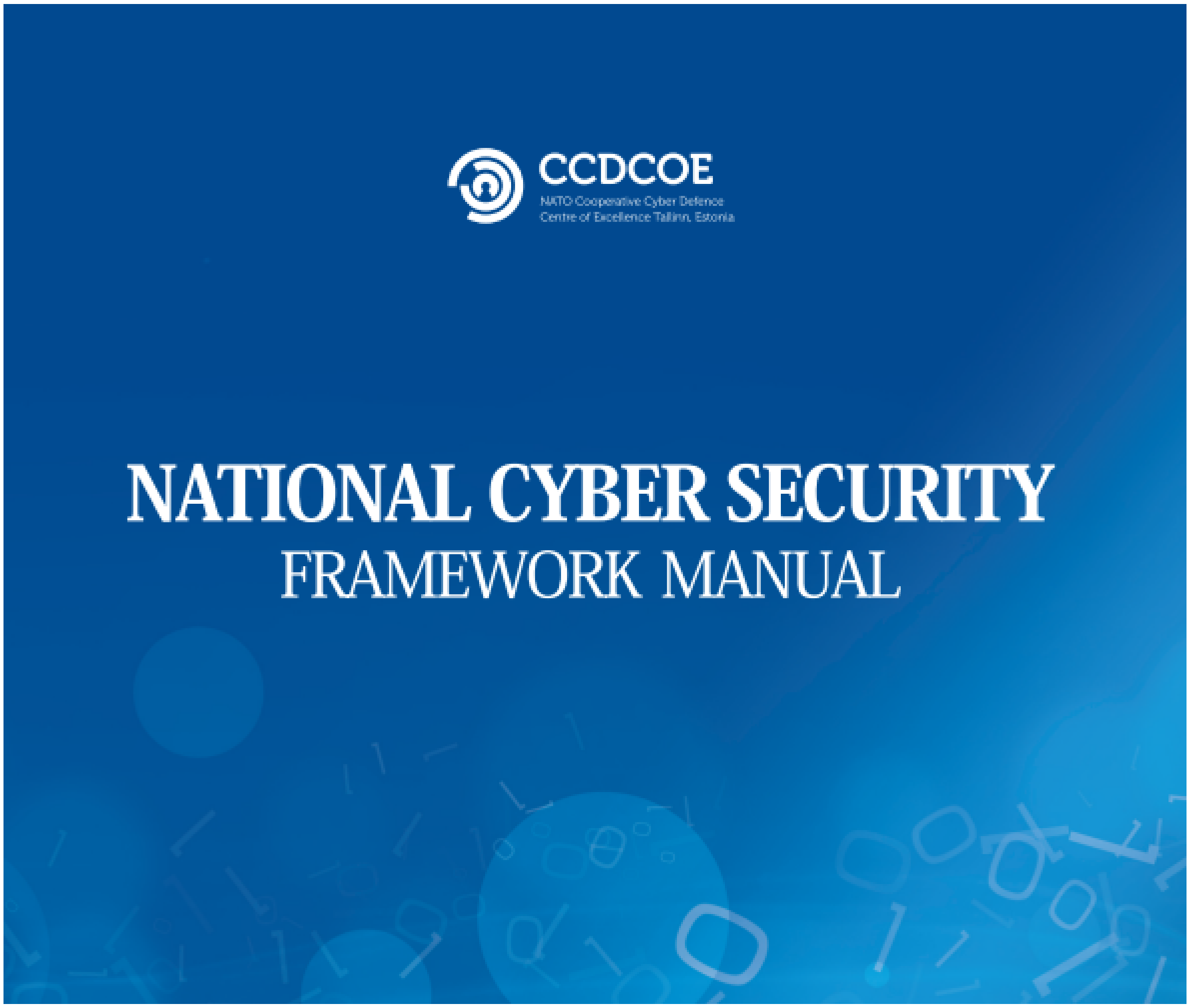
No wonder he was in close contact with military units.

Team Cymru also mentions and boasts of its "network mapping" capabilities in many of its commercial presentations to private companies. In some presentations, it is understood that it is also injured from fragment analysis of L4. Flow monitors in their products are integrated into the desired interface. This applies to both entry and exit points of the interface and can also interact with the route table.

It is striking that Team Cymru's telemetry data is used in the method disclosures of the spyware company Candiru, which targets many journalists with the Chrome/zero-day vulnerability. Pure Signal Recon was also used in this investigation.

In one of the advertising studies, we come across an interesting marketing sentence:
“*Pure Signal Recon unlocks over three months of global Internet telemetry, revealing unmatched levels of critical data about billions of connected nodes, networks, servers and clients, regardless if they are victim, target or threat actor. This data is updated in near real time.*”

The company also collaborated with the United State Space Force, which was established in the past years, as part of the Hack-A-Sat event. The close relationship of the company with many government entities cannot be ignored. The company has also been featured in the NATO National Cyber Security Framework Manual catalog series many times.



CCDCOE
NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

NATIONAL CYBER SECURITY
FRAMEWORK MANUAL

In Team Cymru's showcase, the trigger is stored on Amazon cloud servers. For example:
Ec2-52-22-205-159.compute-1.amazonaws.com **(*PTR*)**

The standard subdomain **track.***.*****, which follows many site link tabs and stabilization, is also used in these company products:
track.cymru.com

The important subdomains of Team Cymru's analysis tools, in which these databases are used, are listed below:

[**38.229.33.199**] →
deaad00.nimbus.cymru.com
fb4f610.nimbus.cymru.com
zeil810.nimbus.cymru.com
suy4c10.nimbus.cymru.com
ce4e440.nimbus.cymru.com
ea99f40.nimbus.cymru.com
vneaj40.nimbus.cymru.com
bcb4650.nimbus.cymru.com
ad53960.nimbus.cymru.com
aa62580.nimbus.cymru.com
fff5880.nimbus.cymru.com
efa8880.nimbus.cymru.com
woii790.nimbus.cymru.com
ae87da0.nimbus.cymru.com
uoseqi0.nimbus.cymru.com
wq0dnm0.nimbus.cymru.com
lc9fho0.nimbus.cymru.com
bb10911.nimbus.cymru.com
ea7ac11.nimbus.cymru.com
cc7ee21.nimbus.cymru.com
bk3tv31.nimbus.cymru.com
ac68451.nimbus.cymru.com
fbb4a51.nimbus.cymru.com
db75561.nimbus.cymru.com
puk0761.nimbus.cymru.com
bde8671.nimbus.cymru.com
fec1881.nimbus.cymru.com
cf59b91.nimbus.cymru.com
lzg72a1.nimbus.cymru.com
cd586d1.nimbus.cymru.com
ee05dd1.nimbus.cymru.com
mpas1h1.nimbus.cymru.com

```
ykct0i1.nimbus.cymru.com
pa13ok1.nimbus.cymru.com
oahyfl1.nimbus.cymru.com
wwtg3s1.nimbus.cymru.com
gii2bs1.nimbus.cymru.com
ce5gws1.nimbus.cymru.com
wwl40t1.nimbus.cymru.com
xtasrt1.nimbus.cymru.com
rerbjv1.nimbus.cymru.com
yuflmy1.nimbus.cymru.com
aad0c02.nimbus.cymru.com
odkel02.nimbus.cymru.com
cbe6e12.nimbus.cymru.com
ho0jx12.nimbus.cymru.com
fb07622.nimbus.cymru.com
af6c532.nimbus.cymru.com
edc7a32.nimbus.cymru.com
ji0ku32.nimbus.cymru.com
af3e282.nimbus.cymru.com
pkdk1b2.nimbus.cymru.com
ce826b2.nimbus.cymru.com
fdd0bb2.nimbus.cymru.com
bc1aac2.nimbus.cymru.com
if1eid2.nimbus.cymru.com
bacacf2.nimbus.cymru.com
objw8i2.nimbus.cymru.com
ndjzpl2.nimbus.cymru.com
px6gvn2.nimbus.cymru.com
jks1yo2.nimbus.cymru.com
jwc2nt2.nimbus.cymru.com
vxri1u2.nimbus.cymru.com
uqhl1u2.nimbus.cymru.com
madd4x2.nimbus.cymru.com
rn8y1z2.nimbus.cymru.com
fbc8c03.nimbus.cymru.com
zgusf23.nimbus.cymru.com
ac92543.nimbus.cymru.com
ecabb43.nimbus.cymru.com
bef3353.nimbus.cymru.com
aaa8553.nimbus.cymru.com
ieig373.nimbus.cymru.com
mwc8573.nimbus.cymru.com
gm4wn73.nimbus.cymru.com
uvv57a3.nimbus.cymru.com
```

ccbe2b3.nimbus.cymru.com
pl9d8c3.nimbus.cymru.com
aoxcsf3.nimbus.cymru.com
ffhyvj3.nimbus.cymru.com
zy0i1p3.nimbus.cymru.com
yoh47q3.nimbus.cymru.com
sfxtiq3.nimbus.cymru.com
Az07gr3.nimbus.cymru.com
th5wwx3.nimbus.cymru.com
zuy9g04.nimbus.cymru.com
jquqx04.nimbus.cymru.com
wybh534.nimbus.cymru.com
dav4944.nimbus.cymru.com
be03b44.nimbus.cymru.com
hg5u054.nimbus.cymru.com

[**38.229.1.199**] →
xx8dkx3.nimbus.cymru.com
ma5r8d1.nimbus.cymru.com
unzxq12.nimbus.cymru.com

[38.229.44.129] →
oldgw01-lo1.ord08.infra.cymru.com

[**38.229.44.130**] →
oldgw02-lo1.ord08.infra.cymru.com

[**38.229.44.131**] →
oldgw03-lo1.ord08.infra.cymru.com

[**38.229.33.5**] →
jabba.cymru.com

[**172.16.7.208**] →
augury-qa.cymru.com

Below are the product access panel entries:
https://augury5.cymru.com/login
https://orbit.cymru.com/login

orbit.cymru.com still redirects to *augury5.cymru.com*.

The company conducts chat meetings via Zoom. The source was revealed by examining: https://chat.cymru.com

It's good to remember this: Most of the institutions and organizations mentioned above have come across similar cases in the past years.

Research and investigations will continue.