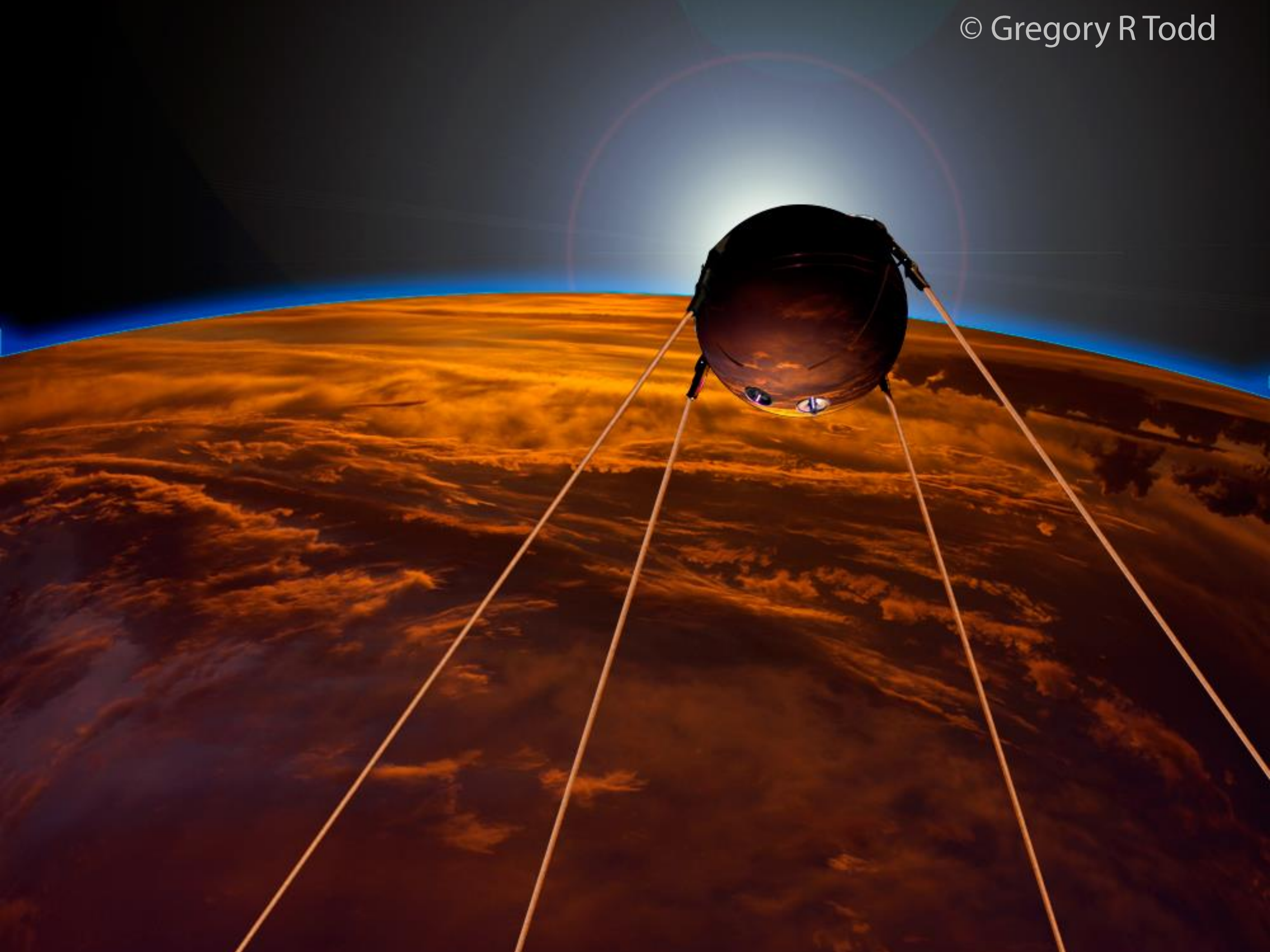
HOU.SEC.CON 4.0

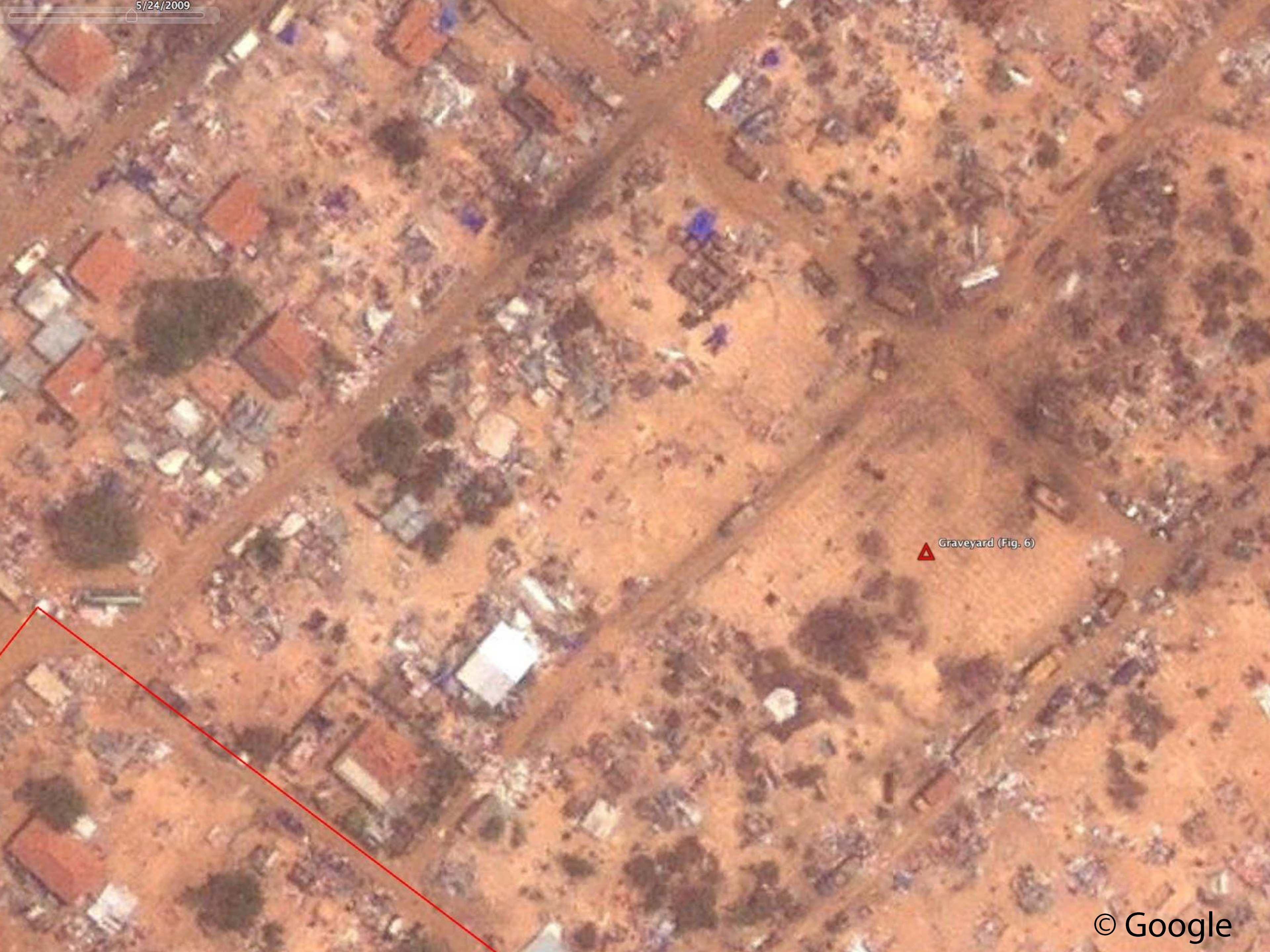
HD Moore | The Security Space Age

HD Moore

- Founder and architect of Metasploit
- Chief research officer for Rapid7

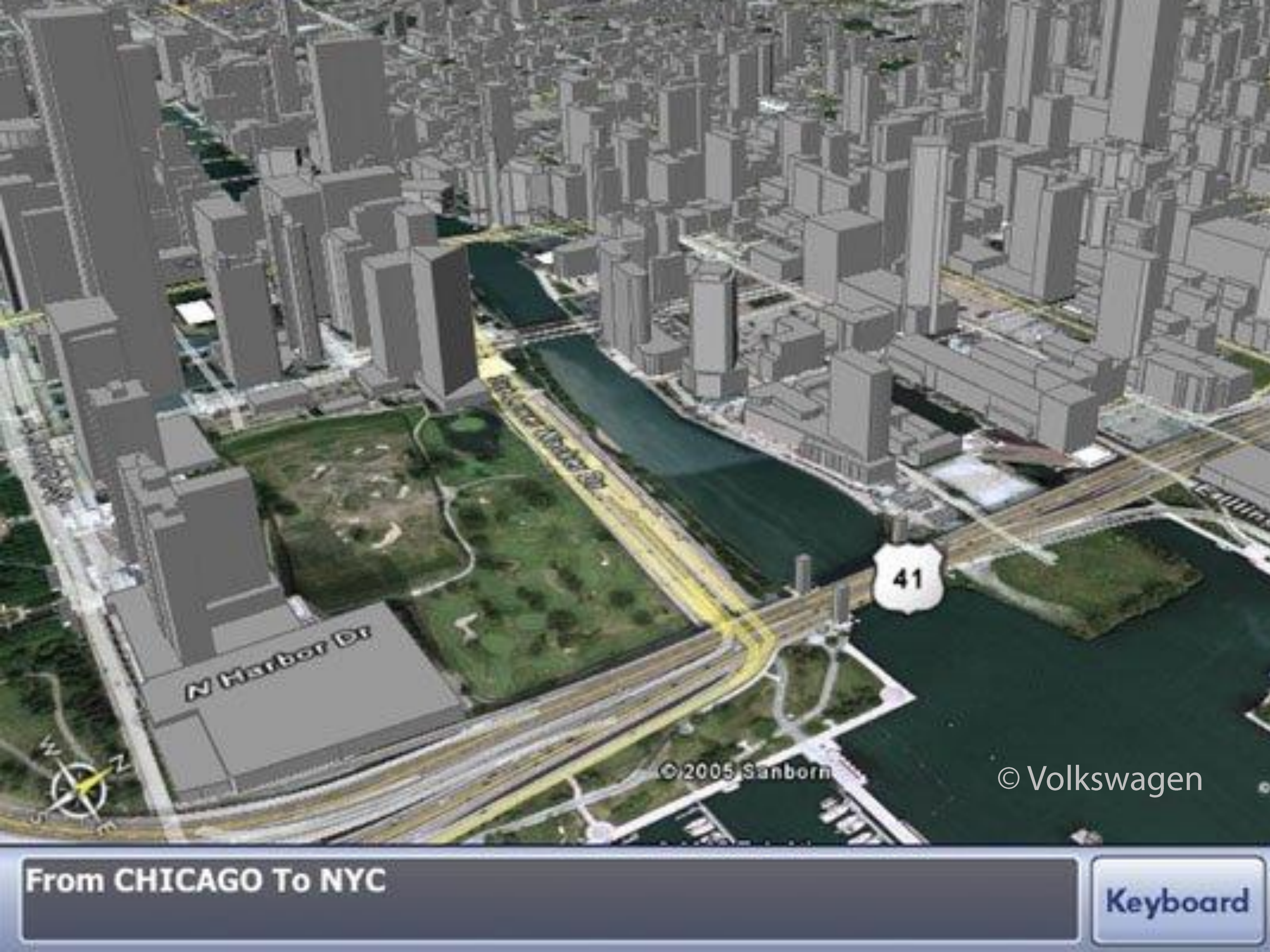


© Mario Bordieri

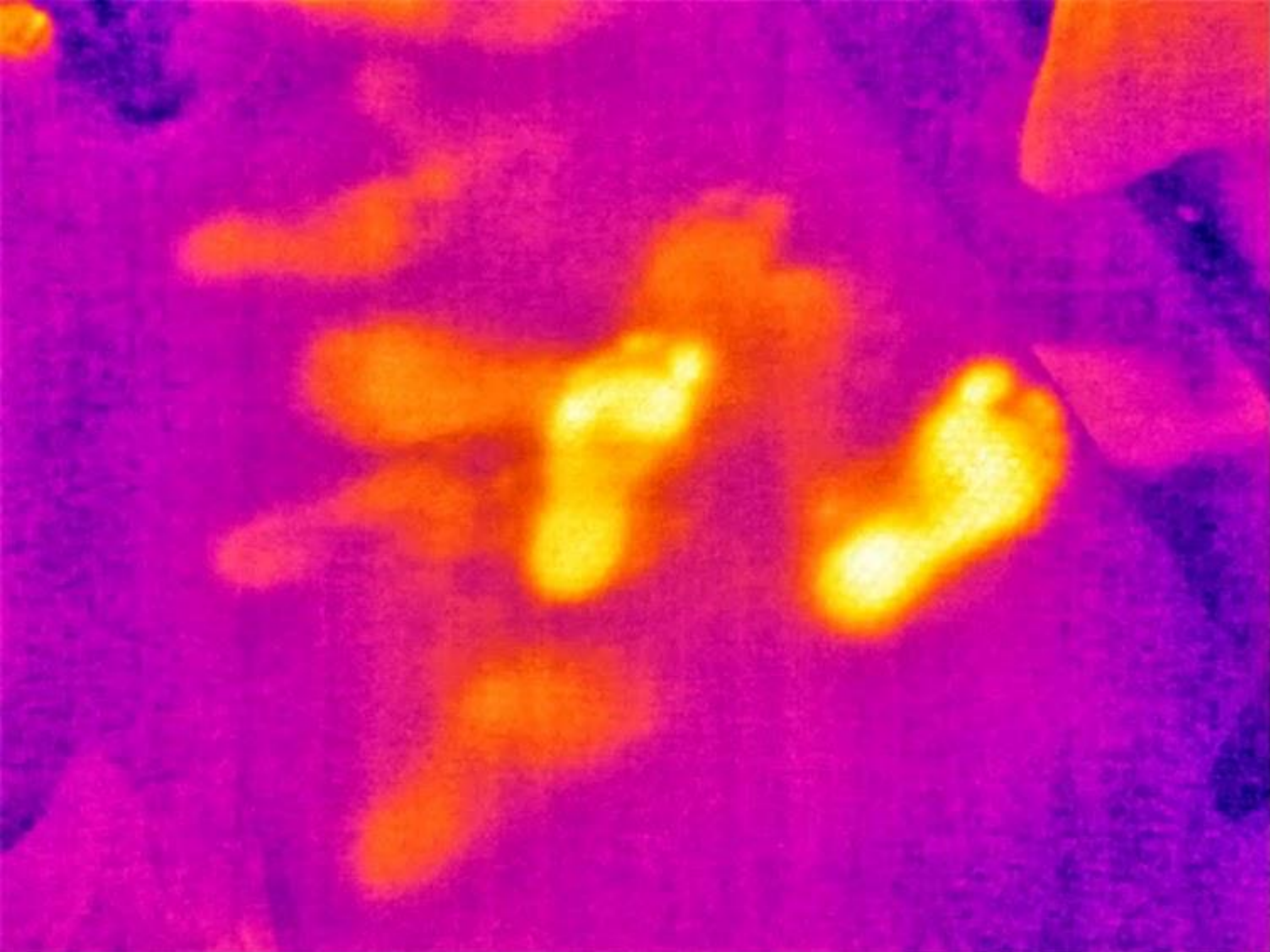


5/24/2009

© Google



From CHICAGO To NYC



© Altemark

GAO

Global Access Operations

The mission never sleeps...

BOUNDLESSINFORMANT

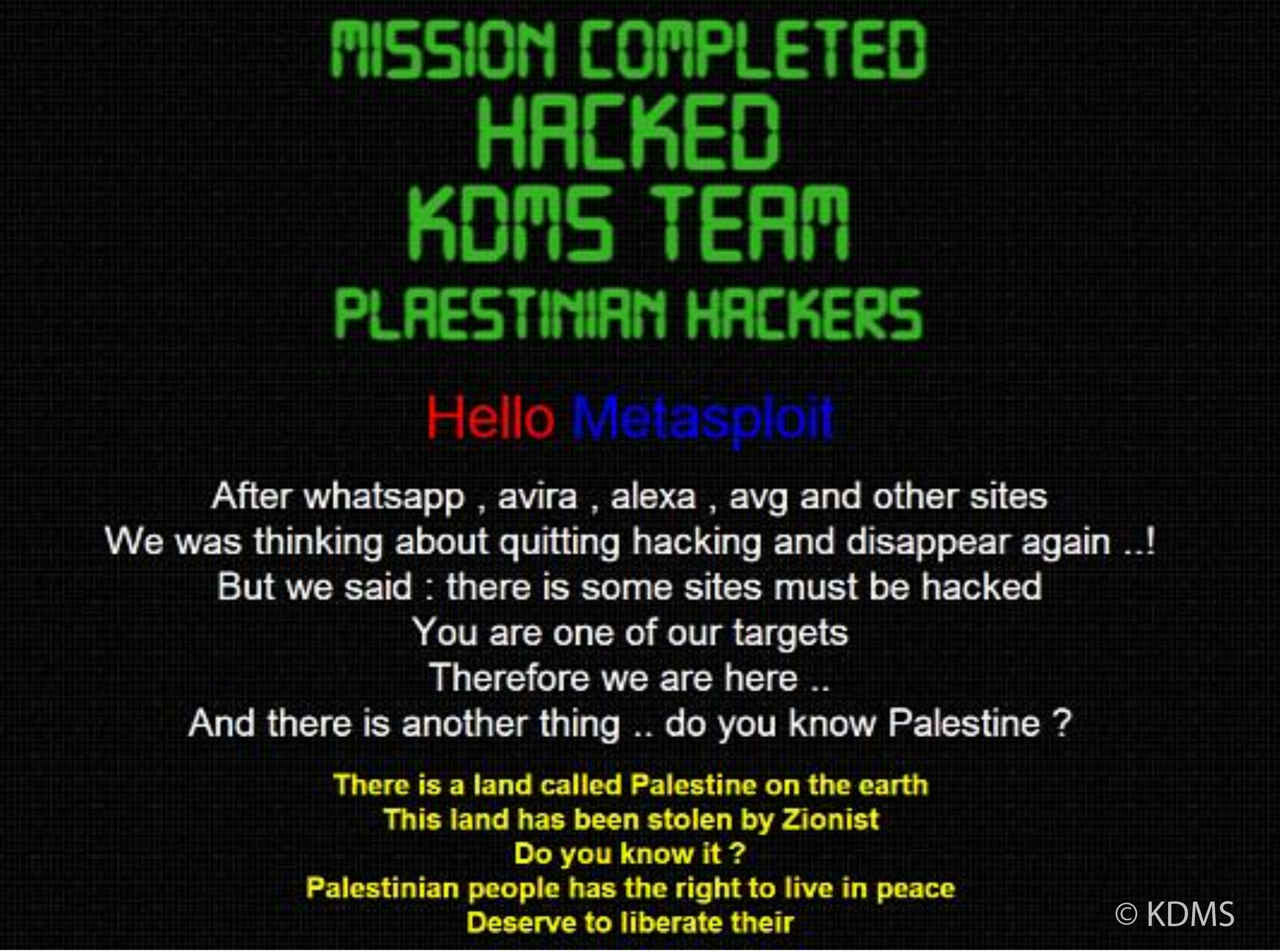
Describing Mission Capabilities from Metadata Records

[redacted]

13 July 2012

© US Army

Sun
789
Linux



MISSION COMPLETED

HACKED

KDMS TEAM

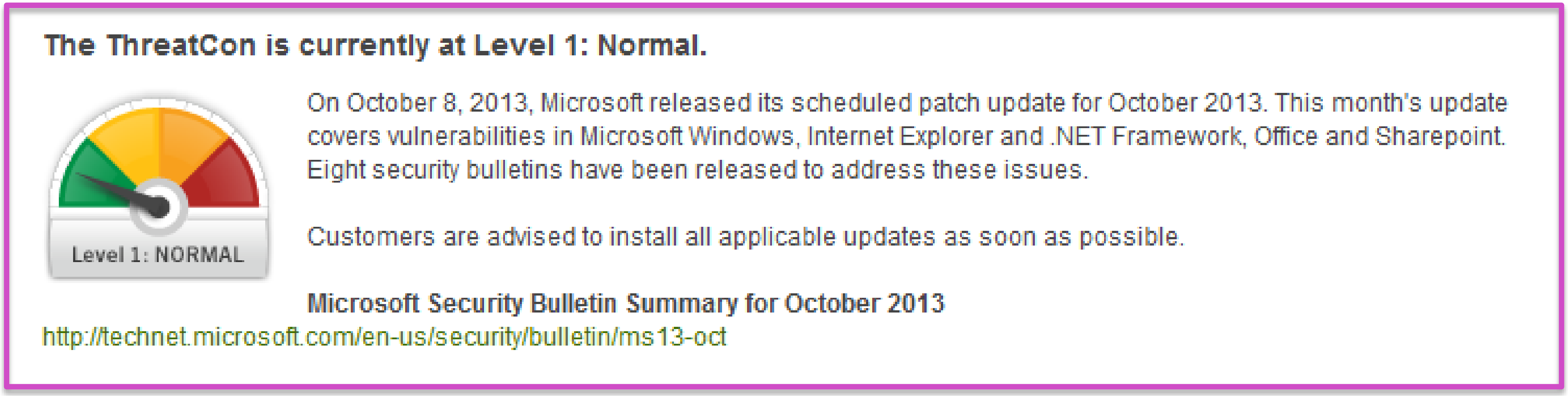
PLAESTINIAN HACKERS

Hello Metasploit

After whatsapp , avira , alexa , avg and other sites
We was thinking about quitting hacking and disappear again ..!
But we said : there is some sites must be hacked
You are one of our targets
Therefore we are here ..
And there is another thing .. do you know Palestine ?

There is a land called Palestine on the earth
This land has been stolen by Zionist
Do you know it ?
Palestinian people has the right to live in peace
Deserve to liberate their

© KDMS

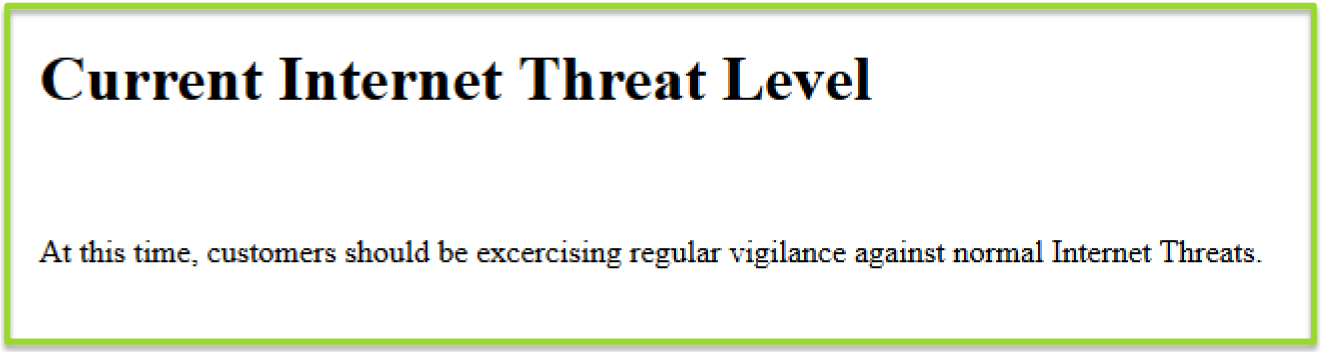


The ThreatCon is currently at Level 1: Normal.

On October 8, 2013, Microsoft released its scheduled patch update for October 2013. This month's update covers vulnerabilities in Microsoft Windows, Internet Explorer and .NET Framework, Office and Sharepoint. Eight security bulletins have been released to address these issues.

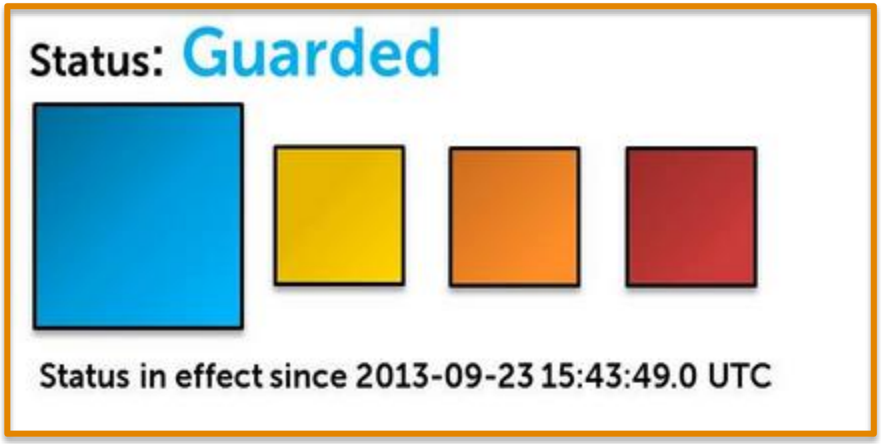
Customers are advised to install all applicable updates as soon as possible.

Microsoft Security Bulletin Summary for October 2013
http://technet.microsoft.com/en-us/security/bulletin/ms13-oct



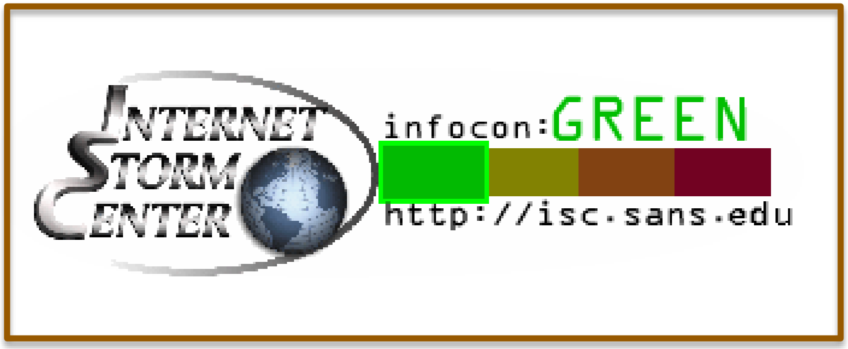
Current Internet Threat Level

At this time, customers should be excercising regular vigilance against normal Internet Threats.



Status: Guarded

Status in effect since 2013-09-23 15:43:49.0 UTC



Internet Storm Center

infocon:GREEN

http://isc.sans.edu

26
3
2

Measuring the Internet

Measurement requires scanning

- Distributed nature makes passive analysis hard
- The NSA isn’t sharing their data feeds
- Scanning is getting way faster

State of Scans

Mass scanning is starting to mature

- Major improvements to scanning tools
- Numerous large-scale scanning efforts
- Scary and not-so-scary precedents

ZMap

U. Michigan team released Zmap

- Send a single probe across IPv4 in 45 minutes
- Detailed research paper with examples
- Development continues at GitHub
- Epic forge-socket support
- http://zmap.io

```
$ zmap -p 80 -o results.txt
```

ZMap: Data Collection

Over 110 internet-wide SSL scans in 12 mos

- Created a detailed view of the SSL ecosystem
- Realtime monitoring of Sandy outages
- Obtained 43 million unique certs

MASSCAN

Errata Security released Masscan

- Scan all of IPv4 for a single TCP port in 3 minutes*
- Leverages 10GbE NICs and PF_RING sockets
- Development continues at GitHub

```
$ masscan 0.0.0.0/0 -p 80
```

Nmap

Nmap 6.40 makes scanning mo-better!

- Performance improvements all around
- Tons of new scripts and fingerprints
- XML + NSE output improvements
- Swiss army knife of scanning

Nmap

Nmap is competitive with the right options

- Combine –sS with –PS for one-pass SYN scans
- Set --min-rate and --min-rtt-timeouts
- Limit retries with –-min-retries

Internet Census 2012

Benign botnet used to scan the internet

- Used over 420,000 devices to scan over 730 ports
- Excellent writeup and a whopping 9Tb of data

SHODAN

Shodan keeps getting better, use it!

- Over three years of internet scan data
- Searchable web interface & API

Challenges

Internet scanning has barriers to entry

- Legal concerns vary by region and attitude
- Scans lead to abuse complaints to ISPs
- Computing and time costs

Status Quo

Internet scanning is a niche field

- Challenges prevent widespread adoption
- Value is centered around research
- Businesses can see it as a threat

Internet Scan Data

Internet scan data is incredibly useful

- Identify and quantify widespread vulnerabilities
- Provide due diligence for vendors & partners
- Market share information for products
- Locate unmanaged corporate assets
- Get a handle on shadow IT

Security is Getting Worse

Hard to find any measurable improvement

- Exposures are getting worse each time we look
- VxWorks WDBRPC exposure is increasing
- UPnP has shown minimal improvements
- DDNS DDoS is bad enough
- SNMP is worse

Time for a Change

This is a rock the community can move

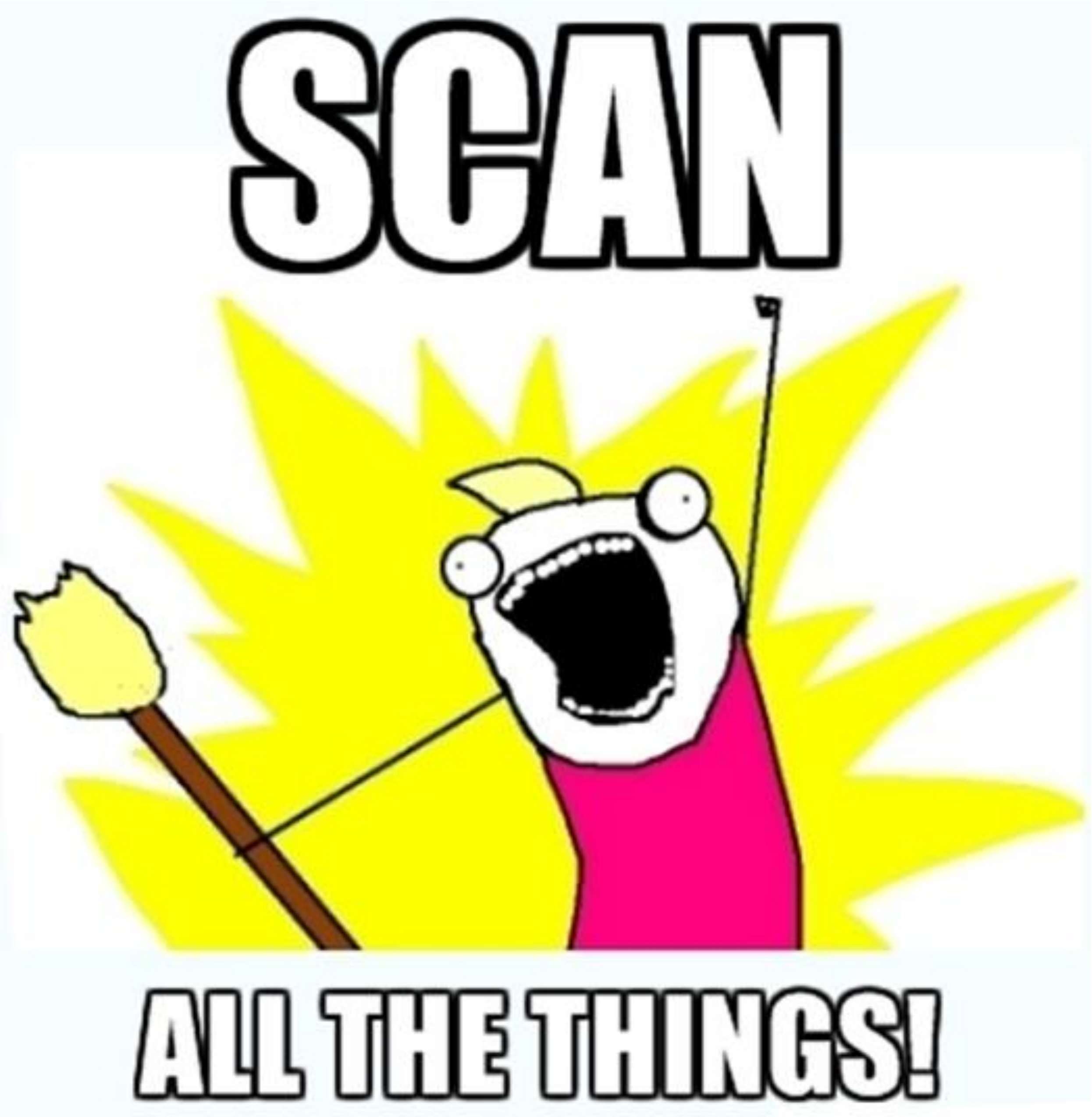
- Demonstrate value to IT, security, and the business
- Drive research based on quantified exposure
- Build awareness around public networks
- Hold vendors and ISPs accountable
- Provide ammo for legal reform

Project Sonar

Community project for internet scans

- Open source tools to simplify scanning
- Open datasets for everyone
- Practical applications

http://miniurl.org/sonar


SCAN
ALL THE THINGS!

Sonar: Scanning

Integration with existing tools

- UDP probes and processing tools for Zmap
- NSE scripts for running with Nmap
- SSL certificate grabbers
- Fast DNS lookup tools

Sonar: Dataset 1

Critical.IO Archive

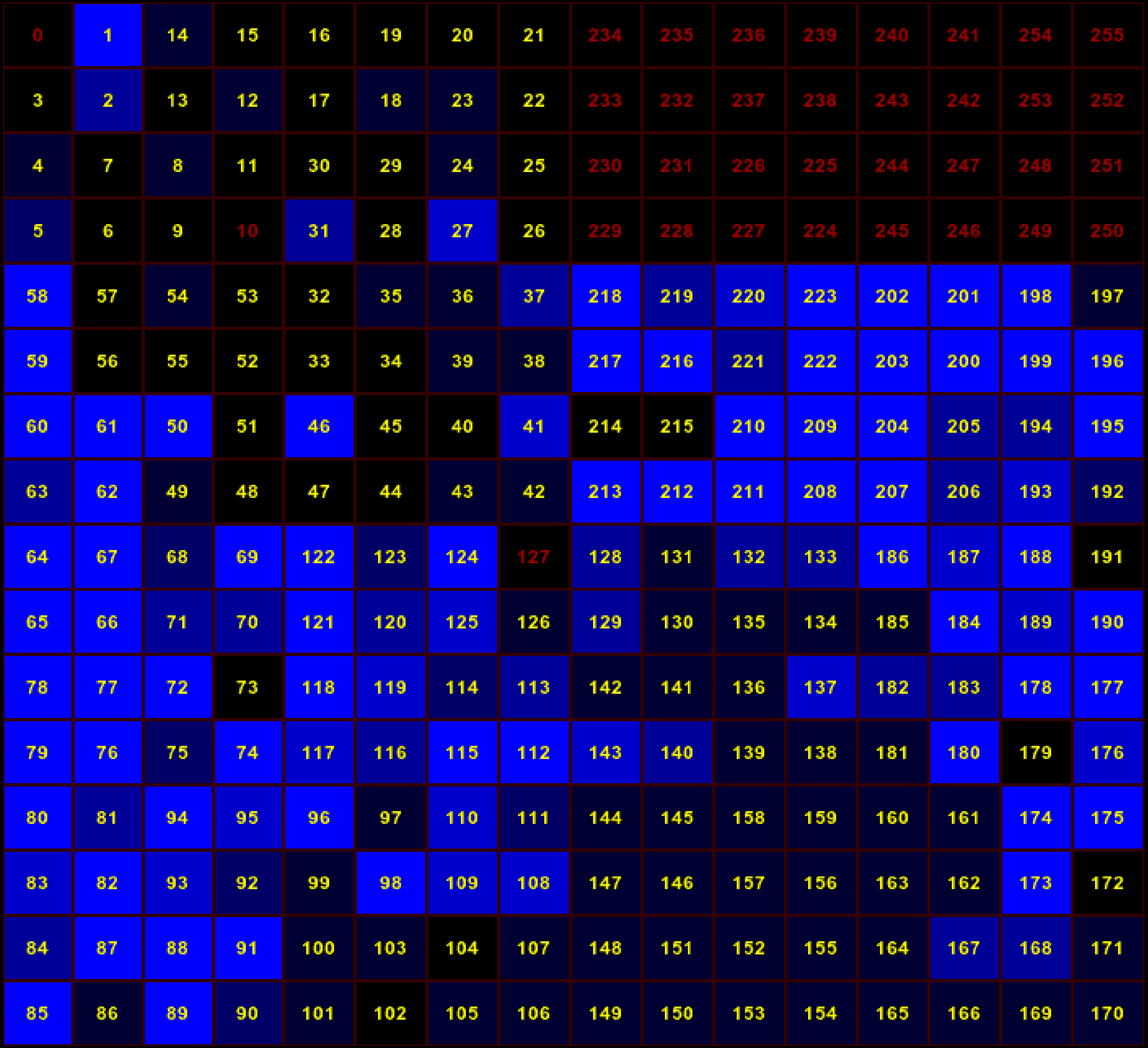
- Parsed banners across 18 services over 10 months
- Current dataset is in compressed JSON
- Historical view of your networks
- Segmented for easy lookups

Sonar: Dataset 1

- 2.4 TB of service fingerprints (355 GB bz2 compressed)
- 1.57 billion records

Management	Email	Discovery	Web
21/tcp	25/tcp	137/udp	80/tcp
22/tcp	110/tcp	1900/udp	443/tcp
23/tcp	143/tcp	5353/udp	8080/tcp
5900/tcp	993/tcp	17185/udp	
3306/tcp	995/tcp		
161/udp			

Port 21



0	1	14	15	16	19	20	21	234	235	236	239	240	241	254	255
3	2	13	12	17	18	23	22	233	232	237	238	243	242	253	252
4	7	8	11	30	29	24	25	230	231	226	225	244	247	248	251
5	6	9	10	31	28	27	26	229	228	227	224	245	246	249	250
58	57	54	53	32	35	36	37	218	219	220	223	202	201	198	197
59	56	55	52	33	34	39	38	217	216	221	222	203	200	199	196
60	61	50	51	46	45	40	41	214	215	210	209	204	205	194	195
63	62	49	48	47	44	43	42	213	212	211	208	207	206	193	192
64	67	68	69	122	123	124	127	128	131	132	133	186	187	188	191
65	66	71	70	121	120	125	126	129	130	135	134	185	184	189	190
78	77	72	73	118	119	114	113	142	141	136	137	182	183	178	177
79	76	75	74	117	116	115	112	143	140	139	138	181	180	179	176
80	81	94	95	96	97	110	111	144	145	158	159	160	161	174	175
83	82	93	92	99	98	109	108	147	146	157	156	163	162	173	172
84	87	88	91	100	103	104	107	148	151	152	155	164	167	168	171
85	86	89	90	101	102	105	106	149	150	153	154	165	166	169	170

Sonar: Dataset 2

SSL Certificates

- All SSL certs on IPv4 port 443 as of September 10th
- Available as raw certs and parsed IP -> Name pairs
- ~33 million records @ 50 GB (16 GB compressed)
- ~8.6 million unique IP->Name pairs (270 MB)

Sonar: Dataset 3

Reverse DNS

- Full reverse DNS for IPv4, regularly updated
- ~1.13 billion records @ 50 GB (3 GB compressed)
- Similar use cases to DeepMagic’s PTR search

Data Portals & Downloads

ZMap & Rapid7 teams are collaborating

- Launching a shared internet scan data portal
- Accepting data from third-parties (you!)
- Includes all datasets already mentioned
- Also 18 months of SSL scans!

http://scans.io

Examples: Research

You can find zero-day with public datasets

- Easy to identify common vulnerabilities
- Look for min/max and anomalies
- Unix pipelines are all you need

Duplicate SSL Certificates

Random things that aren’t random

- Any duplicate SSL key is probably a vulnerability
- Tens of thousands of systems with duplicates
- We need eyes to actually classify these
- Identify vendors and report

SSL Fingerprinting

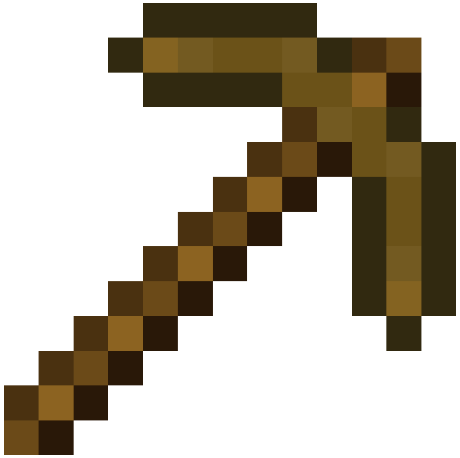
SSL certificates make good fingerprints

- Identify all occurrences of an embedded device
- Locate otherwise hard to identify systems
- Enterprise appliances galore

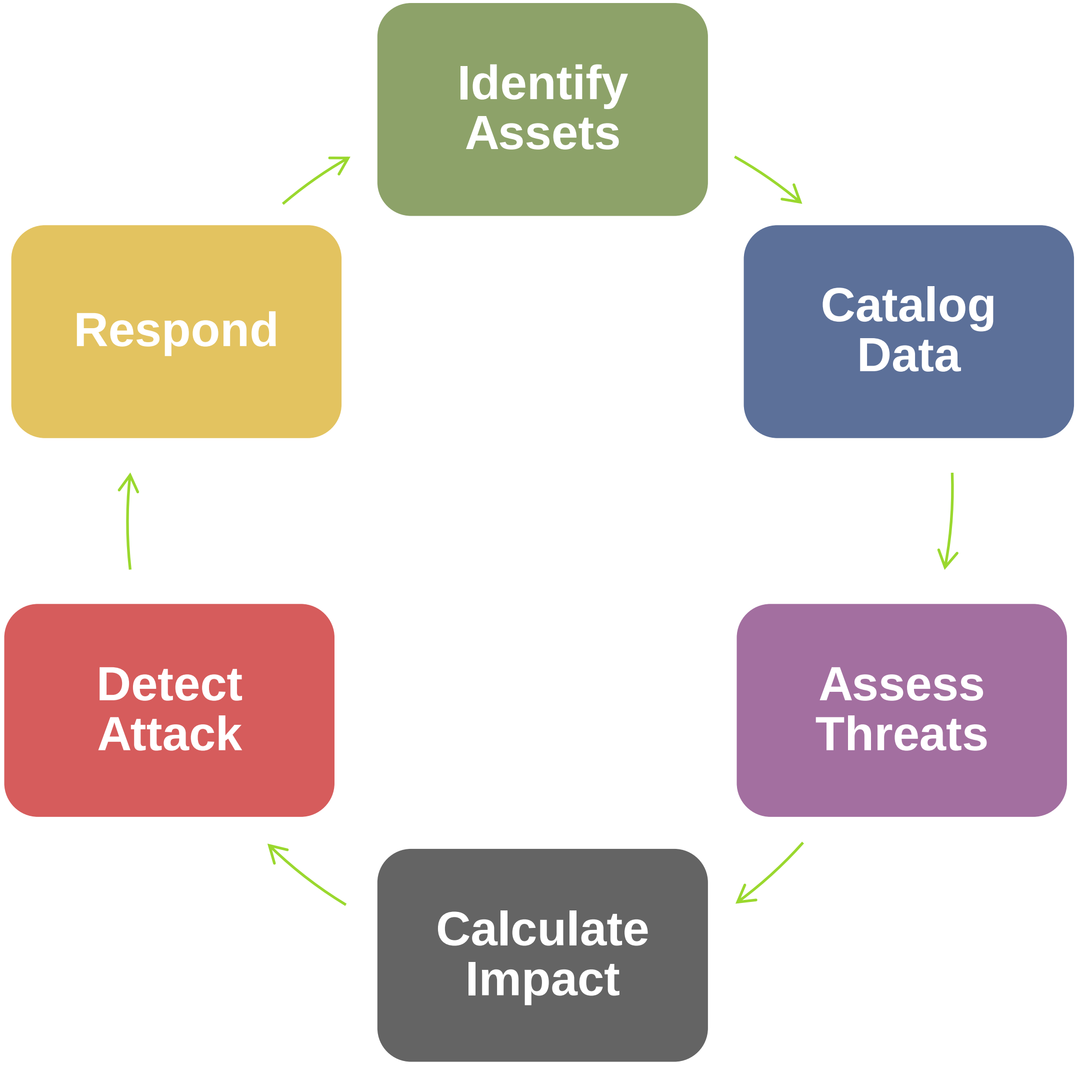
Examples: Infosec

Improving your company’s security

- Identify external assets you may have missed
- Quickly scan massive networks easily
- Historical data helps with response
- Practical data mining



Assets vs Incidents



Asset Discovery (SSL)

SSL certificates are ubiquitous

- Every important site has a SSL certificate
- SSL certificates map to domains

Cloud services often use customer certificates

- Identify undocumented third-party services
- May find 10%+ more than your IT knows about

Asset Discovery (DNS)

Reverse DNS provides an interesting view

- Forward DNS may not match, but reverse is still set
- Find routers, modems, old ISP connections
- Find VPS services, rogue partners, and VARs
- Accidentally the whole intel agency

Quick Risk Assessment

Classify 100,000 nodes in 5 minutes

- Quickly scan a small subset of ports
- Send UDP probes for dangerous services
- Analyze, sort, and prioritize assessment

RAPID7

Q & A

Twitter: **@hdmoore**

Email: **hdm@rapid7.com**

http://miniurl.org/sonar

RAPID7