HIDE AND SEEK

Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries

By Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert

SEPTEMBER 18, 2018
RESEARCH REPORT #113

munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY

UNIVERSITY OF TORONTO

THECITIZENLAB

Copyright

Document Version: 1.0

Suggested Citation

Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert. "Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries," Citizen Lab Research Report No. 113, University of Toronto, September 2018.

Acknowledgements

Bill Marczak's work on this project was supported by the Center for Long Term Cybersecurity (CLTC) at UC Berkeley. This work was also supported by grants to the Citizen Lab from the Ford Foundation, the John T. and Catherine D. MacArthur Foundation, the Oak Foundation, the Open Society Foundations, and the Sigrid Rausing Trust. This work includes data from Censys.

Editing and other assistance provided by Cynthia Khoo, Jeffrey Knockel, Jakub Dalek, Miles Kenyon, Adam Senft, Jon Penney, and Masashi Nishihata.

About the Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto

The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs and Public Policy, University of Toronto, focusing on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security.

We use a "mixed methods" approach to research that combines methods from political science, law, computer science, and area studies. Our research includes investigating digital espionage against civil society, documenting Internet filtering and other technologies and practices that impact freedom of expression online, analyzing privacy, security, and information controls of popular applications, and examining transparency and accountability mechanisms relevant to the relationship between corporations and state agencies regarding personal data and other surveillance activities.

Contents

Contents

Key Findings

- Between August 2016 and August 2018, we scanned the Internet for servers associated with NSO Group's Pegasus spyware. We found 1,091 IP addresses that matched our fingerprint and 1,014 domain names that pointed to them. We developed and used ***Athena***, a novel technique to cluster some of our matches into 36 distinct Pegasus systems, each one which appears to be run by a separate operator.
- We designed and conducted a global *DNS Cache Probing* study on the matching domain names in order to identify in which countries each operator was spying. Our technique identified a total of 45 countries where Pegasus operators may be conducting surveillance operations. At least 10 Pegasus operators appear to be actively engaged in cross-border surveillance.
- Our findings paint a bleak picture of the human rights risks of NSO's global proliferation. At least six countries with significant Pegasus operations have previously been linked to abusive use of spyware to target civil society, including Bahrain, Kazakhstan, Mexico, Morocco, Saudi Arabia, and the United Arab Emirates.
- Pegasus also appears to be in use by countries with dubious human rights records and histories of abusive behaviour by state security services. In addition, we have found indications of possible political themes within targeting materials in several countries, casting doubt on whether the technology is being used as part of "legitimate" criminal investigations.

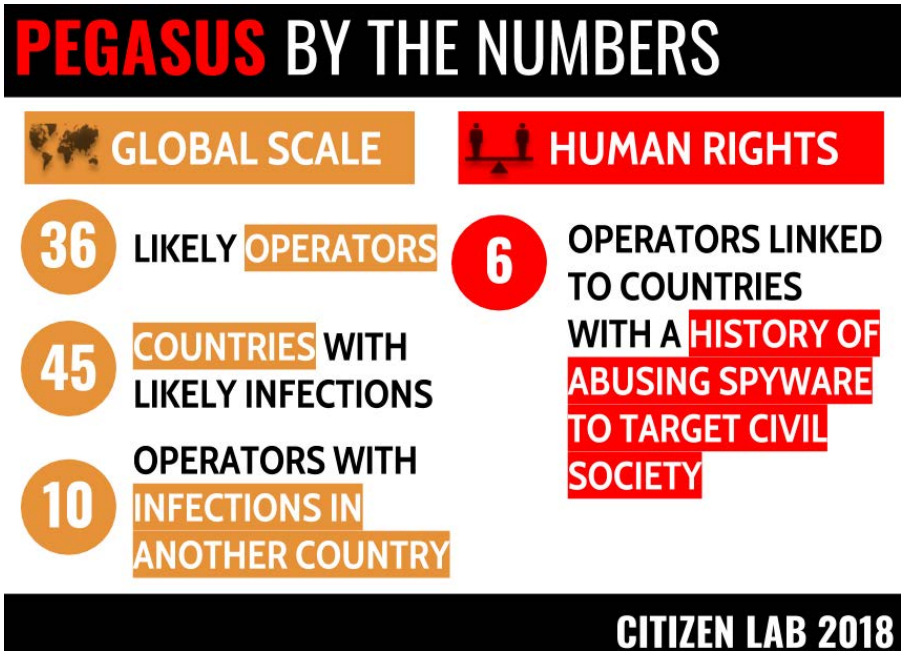

Figure 1: Scope, scale, and context of Pegasus as identified in this report.

1. Executive Summary

Israel-based "Cyber Warfare" vendor NSO Group produces and sells a mobile phone spyware suite called *Pegasus*. To monitor a target, a government operator of Pegasus must convince the target to click on a specially crafted *exploit link*, which, when clicked, delivers a chain of zero-day exploits to penetrate security features on the phone and installs Pegasus without the user's knowledge or permission. Once the phone is exploited and Pegasus is installed, it begins contacting the operator's command and control (C&C) servers to receive and execute operators' commands, and send back the target's private data, including passwords, contact lists, calendar events, text messages, and live voice calls from popular mobile messaging apps. The operator can even turn on the phone's camera and microphone to capture activity in the phone's vicinity.

Figure 2: Diagram from purported NSO Group Pegasus documentation showing the range of information gathered from a device infected with Pegasus. Source: Hacking Team Emails.

Pegasus exploit links and C&C servers use HTTPS, which requires operators to register and maintain *domain names*. Domain names for exploit links sometimes impersonate mobile providers, online services, banks, and government services, which may make the links appear to be benign at first glance. An operator may

have several domain names that they use in exploit links they send, and also have several domain names they use for C&C. The domain names often resolve to cloud-based virtual private servers (we call these *front-end servers*) rented either by NSO Group or the operator. The front-end servers appear to forward traffic (via a chain of other servers) to servers located on the operator's premises (we call these the *back-end Pegasus servers*).

Scanning, Clustering, and DNS Cache Probing

In August 2016, award-winning UAE activist Ahmed Mansoor was targeted with NSO Group's Pegasus spyware. We clicked on the link he was sent and obtained three zero-day exploits for the Apple iPhone, as well as a copy of the Pegasus spyware. We fingerprinted the behaviour of the exploit link and C&C servers in the sample sent to Mansoor, and scanned the Internet for other matching front-end servers. We found 237 servers. After we clicked on the link, but before we published our findings on August 24, NSO Group had apparently taken down all of the Pegasus front-end servers we detected. In the weeks after our report, we noticed a small number of Pegasus front-end servers come back online, but the servers no longer matched our fingerprint. We developed a new fingerprint and began conducting regular Internet scans.

Between August 2016 and August 2018, we detected 1,091 IP addresses and 1,014 domain names matching our fingerprint. We developed and used *Athena*, a novel fingerprinting technique to group most of our results into 36 distinct Pegasus systems, each one perhaps run by a separate operator (**Section 2**).

We next sought to identify *where* these Pegasus systems were being used. We hypothesized that devices infected with Pegasus would regularly look up one or more of the domain names for the operator's Pegasus front-end servers using their ISP's DNS servers. We regularly probed tens of thousands of ISP DNS caches around the world via *DNS forwarders* looking for the Pegasus domain names (**Section 3**).

Our Findings

We found suspected NSO Pegasus infections associated with 33 of the 36 Pegasus operators we identified in 45 countries: Algeria, Bahrain, Bangladesh, Brazil, Canada, Cote d'Ivoire, Egypt, France, Greece, India, Iraq, Israel, Jordan, Kazakhstan, Kenya, Kuwait, Kyrgyzstan, Latvia, Lebanon, Libya, Mexico, Morocco, the Netherlands, Oman, Pakistan, Palestine, Poland, Qatar, Rwanda, Saudi Arabia, Singapore, South

Africa, Switzerland, Tajikistan, Thailand, Togo, Tunisia, Turkey, the UAE, Uganda, the United Kingdom, the United States, Uzbekistan, Yemen, and Zambia. As our findings are based on country-level geolocation of DNS servers, factors such as VPNs and satellite Internet teleport locations can introduce inaccuracies.

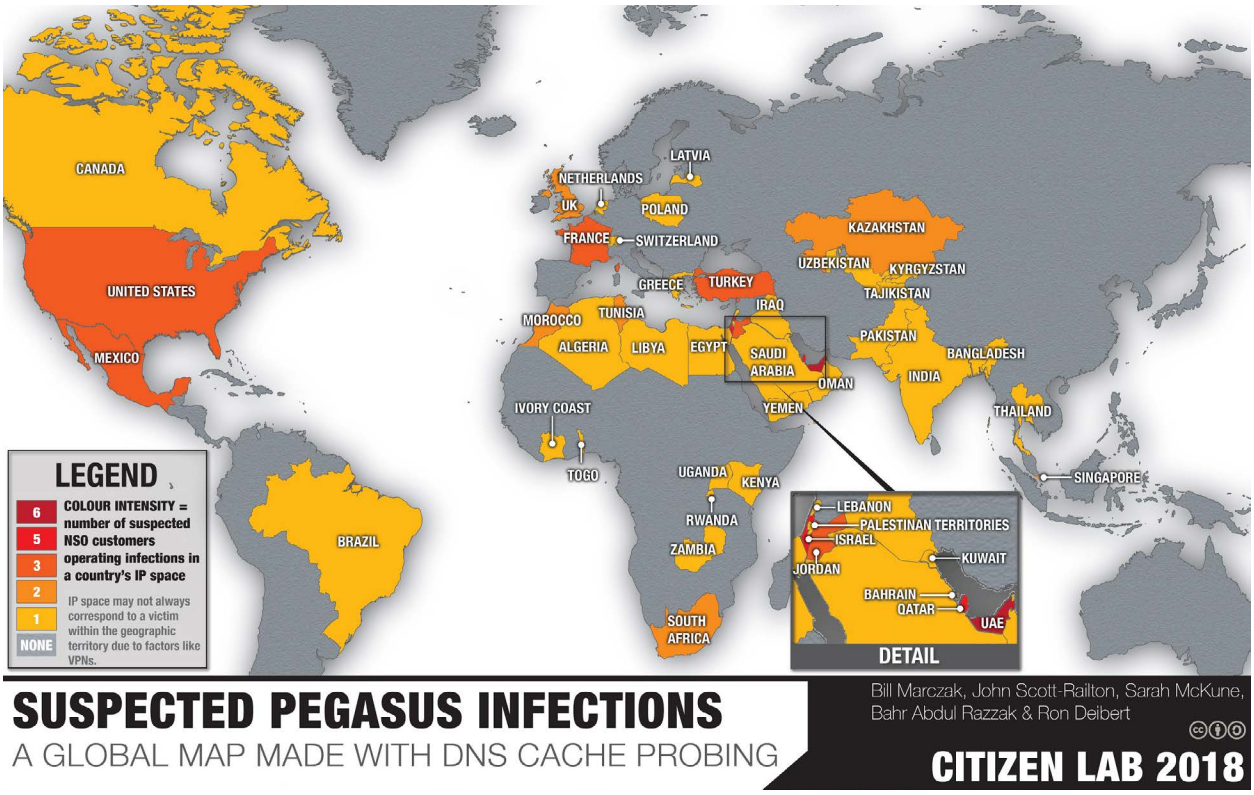

Figure 3: Global map of suspected NSO Pegasus infections.

Mexico

In 2017, we discovered, by retrospectively inspecting their text messages, that dozens of Mexican lawyers, journalists, human rights defenders, opposition politicians, anti-corruption advocates, and an international investigation operating in Mexico were targeted in 2016 with links to NSO Group's Pegasus spyware. The Mexico revelations sparked a major political scandal, *#GobiernoEspía*, and an ensuing criminal investigation, ongoing as of the date of this report. Even after our prior reporting on the abuse of the Pegasus spyware in Mexico, it appears that there are three separate operators who operate predominantly in Mexico as of July 2018.

Gulf Cooperation Council (GCC) Countries

We identify what appears to be a significant expansion of Pegasus usage in the Gulf Cooperation Council (GCC) countries in the Middle East. In total, we identify at least six operators with significant GCC operations, including at least two that appear to predominantly focus on the UAE, one that appears to predominantly focus on Bahrain, and one with a Saudi focus. Three operators may be conducting surveillance beyond the MENA region, including in Canada, France, Greece, the United Kingdom, and the United States.

The GCC countries are well known for abusing surveillance tools to track dissidents. In August 2016, UAE activist Ahmed Mansoor was targeted with NSO Group's Pegasus spyware after previously being targeted with spyware from FinFisher and Hacking Team. Bahrain is noteworthy for compromising journalists, lawyers, opposition politicians, and pro-democracy activists with FinFisher's spyware between 2010 and 2012. In May and June 2018, Amnesty International reported that an Amnesty staffer and a Saudi activist based abroad were targeted with NSO Group's Pegasus spyware. The same operator responsible for that targeting appears to be conducting surveillance across the Middle East, as well as in Europe and North America. Saudi Arabia is currently seeking to execute five nonviolent human rights activists accused of chanting slogans at demonstrations and publishing protest videos on social media.

Other Country Contexts

We identify five operators focusing on Africa, including one that appears to be predominantly focusing on the West African country of Togo, a staunch Israel ally whose long-serving President has employed torture and excessive force against peaceful opposition. The operator in Togo may have used websites with names like "nouveau president" ("new president") and "politiques infos" ("political information") to infect targets with spyware. A separate operator that appears to focus on Morocco may also be spying on targets in other countries including Algeria, France, and Tunisia. We identify several operators operating in Israel: four that appear to operate domestically[1] and one that appears to operate both in Israel, as well as other countries including the Netherlands, Palestine, Qatar, Turkey, and the USA.

1 As NSO Group is based in Israel, some of these might perhaps be demonstration or testing systems

2. Fingerprinting Pegasus Infrastructure

This section describes how we traced Pegasus infrastructure, from our initial discovery in 2016 until the present.

Background

We first began tracking NSO Group's Pegasus spyware after the operators of UAE threat actor Stealth Falcon (later revealed to be UAE cybersecurity company DarkMatter) inadvertently gave us visibility into Pegasus infrastructure by registering a domain name whose homepage included a Pegasus link, using the same email address as a domain for a separate PC spyware product we were tracking. In August 2016, UAE activist Ahmed Mansoor was targeted with Pegasus with a text message sent to his iPhone. We clicked on the link provided in the message and obtained three zero-day exploits for Apple iOS 9.3.3, as well as a copy of the Pegasus spyware. We disclosed the exploits to Apple, which quickly released a patch blocking the Pegasus spyware. According to our scans, all of the Pegasus servers we detected (except for the C&C servers in the sample sent to Mansoor) were shut down at least two days before we published our results.

Fingerprinting in 2016: Decoy Pages

When we sought to build fingerprints for Pegasus infrastructure in 2016, we scanned the Internet for `/redirect.aspx` and `/Support.aspx`, for which Pegasus servers returned *decoy pages*. A decoy page is a page shown when there is an undesired remote landing on a spyware server and is designed to convince the user that they are viewing a normal, benign website. However, because the functionality for showing decoy pages typically resides in the spyware server's code and *likely nowhere else*, it is often trivial for researchers to build fingerprints for decoy pages, and scan the Internet for these fingerprints to identify other servers associated with the same spyware system, including perhaps the servers of *other operators*, if the same spyware system is used by multiple operators.

Fingerprinting in 2017 and 2018: No More Decoys

After our August 2016 report, NSO Group apparently removed the `/redirect.aspx` and `/Support.aspx` decoy pages, and further modified their server code to close an incoming connection without returning any data unless presented with a valid exploit link or other path on the server. This change is in line with changes made by

competitors FinFisher and Hacking Team, after we disclosed how we fingerprinted their hidden infrastructure with decoy pages.

After studying the behavior of several suspected new Pegasus servers, we developed fingerprints Ξ1, Ξ2, and Ξ3, and a technique that we call *Athena*.[2] **Fingerprint Ξ1** is a Transport Layer Security (TLS) fingerprint. **Fingerprints Ξ2** and **Ξ3** represent two different proxying configurations we observed. We considered a server to be part of NSO Group's infrastructure if it matched Ξ1 and also one of Ξ2 or Ξ3. We then used ***Athena*** to group our fingerprint matches into 36 clusters. We believe that each cluster represents an operator of NSO Pegasus spyware, though it is possible that some may represent demonstration or testing systems. As we have done in the past when reporting on vendors of targeted malware, we have chosen to withhold publication of specific fingerprints and techniques to prevent harm that may result from external parties generating a list of NSO Group domains using these methods.

Charting the Rebirth of Pegasus

NSO Group apparently told business associates that our August 2016 report and disclosures of their exploits to Apple *"…disrupted their work for around 30 minutes before they…resumed operations."* Our scanning of NSO Group's infrastructure tells a somewhat different story (Figure 4).

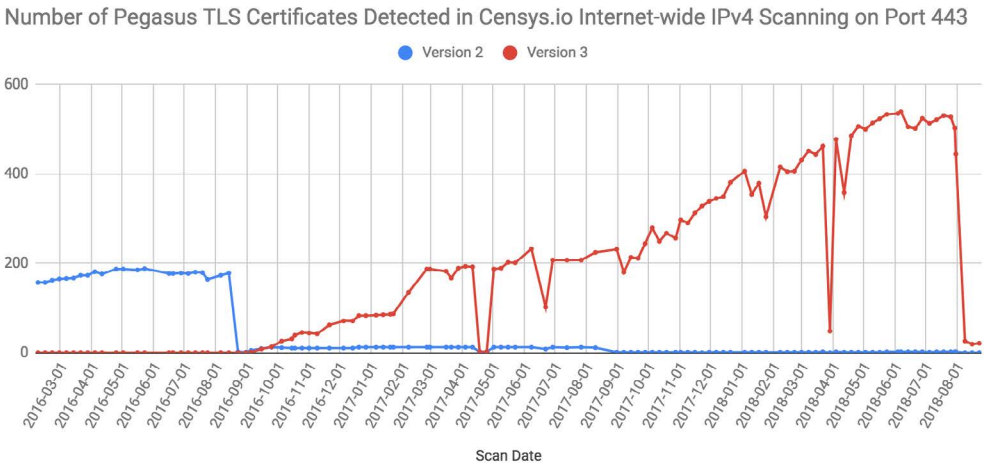

Figure 4: Pegasus servers available over time.

2 According to some accounts of the Pegasus myth, Athena tamed the Pegasus *("For Athena, they say, was the divinity who gave most help to Bellerophontes, and she delivered to him Pegasus, having herself broken in and bridled him.")*

Twelve of the servers that were shut down before we published *Million Dollar Dissident* (we call these **Version 2** servers) were back online in a September 25, 2016 scan and stayed online mostly continuously until an August 10, 2017 scan. These may have been C&C servers for clients that wished to continue monitoring old infections. We saw the first **Version 3** server in a September 5, 2017 scan, less than two weeks after *Million Dollar Dissident*. Approximately one month after *Million Dollar Dissident*, we saw what appeared to be seven operators online. Two months after our report, we saw 14 operators online.

3. DNS Cache Probing Results

*This section describes the results of our DNS Cache Probing study to identify suspected Pegasus infections (see **Section 4** for study details, as well as the definition of a "suspected infection").*

Background

We used the technique that we call *Athena* to cluster the IP addresses that matched our Pegasus fingerprints into what we believe are 36 distinct *operators*; each operator makes use of multiple IP addresses. We give each operator an **Operator Name** drawn from national symbols or geographic features of the country or region that appears to be targeted. For each IP address used by the operator, we extracted a domain name from its TLS certificate. We coded the domain names to generate a **Suspected Country Focus** and assessed whether there were **Political Themes** in the domains, which might suggest politically motivated targeting. We then performed DNS cache probing to generate a list of countries in which there are **Possible Infections** associated with the operator.

Operators Focusing on the Americas

We identified five or six operators that we believe are operating in the Americas.

One operator that we call MACAW may be focused on Honduras or neighboring countries because it made use of two interesting domain names showing a possible link to Honduras (*politica504[.]com* and *eltiempo-news[.]com*). However, our DNS cache probing technique did not identify any suspected infections relating to this system.

At the time of our June 2017 Reckless Exploit report about the abuse of NSO Group's Pegasus spyware in Mexico, there were four operators using domain names that suggested a link to Mexico: RECKLESS-1, RECKLESS-2, PRICKLYPEAR, and AGUILAREAL. RECKLESS-1 and RECKLESS-2 employed some domain names containing political themes (RECKLESS-1 used *universopolitico[.]net* and *animal-politico[.]com*; RECKLESS-2 used *noticiaspoliticos[.]com* and *politicoportales[.]org*). Operators RECKLESS-1 and RECKLESS-2 are so named because they were swiftly and completely shut down following publication of our report. Operators PRICKLYPEAR and AGUILAREAL were partially shut down: two or three servers for each remained online. One month after publication, in July 2017, the first domain names for a new operator, MAYBERECKLESS, that would focus on Mexico were registered. The MAYBERECKLESS domains began matching our fingerprint in September 2017. MAYBERECKLESS may be a continuation of RECKLESS-1 or RECKLESS-2. Also in September 2017, the remaining servers from PRICKLYPEAR and AGUILAREAL were supplemented with new servers.

Operator name	Dates operator was active	Suspected country focus	Political themes?	Suspected infections
RECKLESS-1	Sep 2016 – Jun 2017	Mexico	Yes	–
RECKLESS-2	Oct 2016 – Jun 2017	Mexico	Yes	–
MAYBERECKLESS	Sep 2017 – present	–	–	Mexico
PRICKLYPEAR	Oct 2016 – present	Mexico	–	Mexico, USA (Arizona)
AGUILAREAL	Sep 2016 – present	Mexico	–	Mexico
MACAW	Nov 2017 – present	Honduras	Yes	–

Operators Focusing on Africa

We identified five operators that we believe are focusing on Africa. One operator that we call REDLIONS uses frontend domains that appear to be almost exclusively written in the French language, including two politically themed domains (*politiques-infos[.]info* and *nouveau-president[.]com*). We found DNS cache probing hits for REDLIONS in Togo. Because we did not perform our DNS cache probing study until July 2018, we did not have the opportunity to probe one operator, AK47, which shut down in July 2017. Operators ATLAS and GRANDLACS also made use of politically themed domains (ATLAS used *revolution-news[.]co* and GRANDLACS used *politicalpress[.]org*).

Operator name	Dates operator was active	Suspected country focus	Political themes?	Suspected infections
REDLIONS	Mar 2017 – present	–	Yes	Togo
ATLAS	Aug 2017 – present	Morocco	Yes	Algeria, Cote d'Ivoire, France, Morocco, Tunisia, UAE
GRANDLACS	Jun 2017 – present	Great Lakes region of Africa	Yes	Kenya, Rwanda, South Africa, Uganda
MULUNGUSHI	Feb 2018 – present	Zambia	–	South Africa, Zambia
AK47	Dec 2016 – Jul 2017	Mozambique	–	–
MACAW	Nov 2017 – present	Honduras	Yes	–

Operators Focusing on Europe

We identified five operators that we believe are focusing on Europe. Two systems that we call TURUL and CHEQUY appear to have a Hungarian and Croatian focus in their frontend domain names, but we did not find any DNS cache probing hits for these systems.

Operator name	Dates operator was active	Suspected country focus	Political themes?	Suspected infections
ORZELBIALY	Nov 2017 – present	Poland	–	Poland
EDELWEISS	Jul 2017 – present	Switzerland	–	Switzerland
5LATS	Mar 2018 – present	Latvia	–	Latvia
TURUL	Feb 2018 – present	Hungary	–	–
CHEQUY	Nov 2016 – present	Croatia	–	–
MACAW	Nov 2017 – present	Honduras	Yes	–

Operators Focusing on the Middle East

We identified 12 operators that we believe are focusing on the Middle East. One operator, PEARL, appears to be focused on Bahrain. One operator, KINGDOM, was behind the recent targeting of an Amnesty staffer and a Saudi Arabian activist abroad. Operator PEARL used politically themed domain names including *shia-voice[.]com* (referring to a politically repressed religious group in Bahrain) and *14-tracking[.]com* (perhaps referring to the February 14 Youth Coalition, a group leading some anti-government protests), and operator FALCON used *nomorewarnow[.]com*.

Operator name	Dates operator was active	Suspected country focus	Political themes?	Suspected infections
PEARL	Jul 2017 – present	Bahrain	Yes	Bahrain, Qatar
FALCON	Oct 2016 – present	UAE	Yes	UAE
BABYFALCON	May 2018 – present	GCC Region	–	UAE
MAYBEFALCON	Sep 2016 – present	–	–	UAE
BLACKBIRD	Sep 2016 – present	–	–	Greece, Jordan, Kuwait, Libya, Qatar, UAE, UK, USA, Yemen
KINGDOM	Oct 2017 – present	Saudi Arabia	–	Bahrain, Canada, Egypt, France, Iraq, Jordan, Lebanon, Morocco, Qatar, Saudi Arabia, Turkey, UK
MIDDLE	Sep 2016 – present	–	–	France, Jordan, Lebanon, Oman, Qatar, Tunisia, Turkey, UAE
OLIVE-1	Jun 2017 – present	–	–	Israel
OLIVE-2	Aug 2017 – present	–	–	Israel
OLIVE-3	Dec 2016 – present	–	–	Israel
OLIVE-4	Oct 2016 – present	–	–	Israel
DOME	Mar 2018 – present	–	–	Israel, Netherlands, Palestine, Qatar, Turkey, USA

Operators Focusing on Asia

We identified five operators that we believe are focusing on Asia. One operator, GANGES, used a politically themed domain *signpetition[.]co*.

Operator name	Dates operator was active	Suspected country focus	Political themes?	Suspected infections
CHANG	Jan 2018 – present	Asia	–	Thailand
GANGES	Jun 2017 – present	–	Yes	Bangladesh, Brazil, Hong Kong, India, Pakistan
MERLION	Dec 2016 – present	–	–	Singapore
TULPAR	Feb 2017 – present	Kazakhstan	–	Kazakhstan
SYRDARYA	Sep 2016 – present	Uzbekistan	–	Kazakhstan, Kyrgyzstan, Tajikistan, Turkey,
Uzbekistan	Nov 2017 – present	Honduras	Yes	–

Highly Customized Operators with Unclear Focus

We identified three operators with an unclear focus, which all appeared to use a large degree of customization in their operations.

Operator **SUPERSIZE** (active Sep 2016 – present) had by far the largest Pegasus deployment based on number of domain names; we found 118 domain names belonging to **SUPERSIZE**. We found interesting DNS cache hits in Israel and Bahrain, but did not have enough information to determine whether these might be suspected infections. It may be the case that SUPERSIZE was monitoring relatively few people with a relatively large amount of infrastructure, or that some of SUPERSIZE's targets may have been outside areas we could measure with DNS cache probing, or that SUPERSIZE was operating in an especially stealthy manner with targets under sporadic, rather than continuous, surveillance.

Operator **SNEAK** (active Oct 2016 – present) had infrastructure that appeared to reflect a high level of customization, including running C&C servers on nonstandard ports, and making use of dynamic DNS services. SNEAK was the operator that accidentally reused some of its old infrastructure, facilitating our continued visibility into NSO Group's infrastructure after our *Million Dollar Dissident* report. We found interesting DNS cache hits on this system in Syria, Lebanon, Qatar, the Netherlands, and the United States, but did not have enough information to determine whether these might be suspected infections.

Operator **PARTY** (active May 2017 – present) used domain names with extremely long TTLs. We found interesting DNS cache hits on this system in Syria and Lebanon, but did not have enough information to determine whether these might be suspected infections.

4. DNS Cache Probing Technique

This section describes our DNS Cache Probing technique.

Background on DNS and Cache Probing

When a user (or a computer program) instructs a computer or mobile device to communicate with a domain name (e.g., www.citizenlab.ca), the device first sends

a request to a Domain Name Service (DNS) server, in order to learn the IP address corresponding to the domain name. By default, the device communicates with a DNS server maintained by the ISP or telecom company to which the device is connected.

DNS servers *cache* mappings between IP addresses and domain names temporarily, typically for a duration specified by the owner of the domain name (e.g., 300 seconds). When a device looks up a domain name that is not in the server's cache, the server contacts other DNS servers to resolve the domain name *"recursively"* and then stores the record in the cache. When a device looks up a domain name that is already in the server's cache, the server returns the record from the cache, along with a *time to live (TTL)* value, that indicates when the server will expire the record from the cache. If the TTL value returned by the server is less than that set by the owner of the domain, then it is likely that the record returned by the DNS server was present in the server's cache, and thus was looked up by some *other* ISP user relatively recently.

One can also send a query to a DNS server with the *Recursion Desired* flag set to 0 (called a *nonrecursive query*), indicating to the server that it should only consult its cache before responding; if the record is not in the cache, the server should not contact other servers to attempt to resolve the domain and should not add anything to its cache. Some DNS servers may choose to not respect this flag.

Sending queries (whether nonrecursive or recursive) to a DNS server for the purpose of observing less-than-full TTLs is a measurement technique called *DNS cache probing* or *DNS cache snooping*. The author of the original presentation of DNS cache probing in 2004 framed it as detrimental to security and privacy and proposed that operators of DNS servers, such as ISPs, should block DNS queries not originating from their own network. Implementing such a precaution would make it harder for a single observer to directly probe caches of DNS servers. A 2006 investigation of a botnet C&C server employed DNS cache probing to investigate prevalence of botnet infections; the authors in that case appear to have probed DNS servers that were *authoritative* for some domain, rather than DNS forwarders.

Even in cases where ISPs block requests to their DNS servers from non-ISP-users, it is sometimes possible to probe the DNS servers' caches, by using *open DNS forwarders* on the ISP's network. An open *DNS forwarder* is a service that accepts queries from any Internet user, and forwards the query, unmolested, perhaps to an ISP server,

which then responds to the forwarder, which in turn responds to the user. From the perspective of the ISP's DNS server, the submitter of the query (the forwarder) is on the ISP's network. Open DNS forwarders may be running on improperly configured routers or IoT devices.

Note: Ethics of DNS Cache Probing

In keeping with the growing emphasis on ethics in network measurement research, we considered the impacts of our technical activities on persons that are not the targets of our research, and sought to minimize the likelihood of any disruption. Notably we examined the possibility of costs to users, service disruption, or unwanted warnings from their ISPs. We believe that this research was conducted in a manner that mitigates these risks, and serves the public interest.

Firstly, we considered the possibility that users might incur costs or service disruption as a result of our DNS Cache Probing. We believe that this is a highly unlikely outcome, given the small number of requests made during the activity. As deployed, the technique results in fewer than one request per second per IP address, and thus is less than one kilobyte per second. The total traffic is thus less than 100 megabytes per day. To further minimize load on the *authoritative* name servers for the domains that we are probing, we use *nonrecursive* queries only. As a result, we do not anticipate costs incurred by users, or bandwidth degradation.

We determined that it was unlikely that users would receive unwelcome inquiries from their ISPs, or other authorities, as the result of our DNS cache probing. Certainly, open DNS forwarders are a major Internet security risk, as they may be employed in DNS amplification DDoS attacks. Such high-volume attacks might come to the notice of ISPs or other authorities and trigger inquiries or sanction by ISPs. DNS Cache Probing, in contrast, is a very low-volume activity. If an open DNS operator has not already received a contact from their ISP, we think it very unlikely that this technique will trigger contacts, since it does not look 'attack-like.'

At the time of writing, we are unaware of any evidence of DNS Cache Probing used in malicious real-world attacks. As the technique of DNS Cache Probing continues to be developed as a research tool, it will be important to ensure that it continues to be used in ways that do not present privacy and security concerns.

Finding Suitable DNS Forwarders

We first develop a list of suitable DNS forwarders. We run three tests to answer the following questions:

1) **Does the forwarder appear to use resolvers that honour nonrecursive queries?** We send a nonrecursive query for a randomized subdomain of a domain we control and check if we get a response. The randomized subdomain resolves to an IP but should not be in any cache. We check each IP twice; if we ever get a correct answer, then the IP does not honour nonrecursive queries.
2) **Which resolvers does the forwarder use?** We run a customized nameserver for a domain we control; the nameserver returns the source IP of an incoming DNS query as one of the answers in the response. We query each IP 10 times with a recursive query for a randomized subdomain of the domain we control and collect the set of IPs returned by our nameserver.
3) **Is the forwarder likely to have access to an interesting cache?** We query each IP 10 consecutive times with a recursive query for *google.com*. If an IP returns a response with an IP in Google's autonomous system (AS #15169) at least once, then the forwarder may have access to an interesting cache.

A DNS forwarder is *suitable* if:

- It appears to honour nonrecursive queries.
- The forwarder appears to only ever forward requests to resolvers in a single Autonomous System (AS). We exclude forwarders that use resolvers in multiple ASes because when such a forwarder shows a DNS cache hit, we do not know in which AS the DNS cache hit actually occurred.
- The (single) AS of the forwarder's resolvers is designated as "Transit/

Access" by CAIDA's AS Classification dataset. This helps avoid some cloud providers and shared *DNS providers* like Google, OpenDNS, Yandex, CloudFlare, etc.

- The AS of the forwarder's resolvers is not equal to any AS where we found a match for an NSO Group server.
- The forwarder is not itself a resolver; in other words, the forwarder IP does not appear amongst the resolvers.
- The forwarder is likely to have access to an interesting cache.

Each time we scanned, our list included ~38,000 suitable forwarders, excluding forwarders in China.

Understanding DNS Cache Probing False Positives

DNS cache probing can produce *false positives*, i.e., the DNS cache probing technique reports that the domain is in the cache, when it is in fact not in the cache, or when we *caused* it to be in the cache. This can happen in the following three cases:

1) A DNS forwarder does not honor nonrecursive queries all of the time; it may forward some subset of our queries to a resolver that does not honor nonrecursive queries. This can result in our query *adding the domain to the cache*.
2) A DNS forwarder might return the entry that we added to the cache in (1). This can happen even for DNS forwarders that do honour nonrecursive queries 100% of the time.
3) Automated processes or curious researchers may observe our DNS cache probing and send DNS queries for the domain names we are probing; this may add the domain names to caches we are probing.

We conducted several control experiments to determine how best to exclude false positives. In our control experiments, we selected 50 domain names with a *wildcard record* and an authoritative TTL of at least 300 seconds, then generated a random string to use as a subdomain, and continuously queried all 50 domains (with the subdomain) on all resolvers once roughly every 300 seconds in a fixed order, at a rate ensuring each domain was queried at least once every 300 seconds. We ran the experiment for 24 hours.

Any results we received during the control experiments we treated as false positives. We developed a set of heuristics to reduce the false positive rate to 0 in these experiments, with the idea that these same heuristics might help us eliminate many false positives from our DNS cache probing study of the spyware domains. These are the conditions we applied to eliminate false positives from our results:

1) **Exclude duplicate observations of the same lookup:** For each DNS server response, we check to see if the observation is a *duplicate*. Specifically, if a response for a given domain name was preceded by a response (*from any DNS forwarder*) for that same domain name n seconds ago, and the TTL of the prior response differed by *n* (± 2) from the present response, then we excluded the present response.

2) **Exclude possible duplicate observations even if clocks run at an incorrect rate:** For each ASN, we excluded a record if its TTL was less than or equal to the immediately prior record for that domain returned by any DNS forwarder for the same ASN (or IP). We implemented this condition because for some ASNs, we identified monotonically nondecreasing sequences of TTLs (for domains with large TTLs) that appeared to correspond with clocks running at incorrect rates, and suspected that these may have been false positives.

3) **Exclude any observation with an improper TTL:** We exclude all observations with TTLs larger than the TTL set by the domain name's authoritative DNS server (authoritative TTL), as well as all observations with TTLs within 2 of the authoritative TTL, as well as all observations with popular fixed TTL values (0, 1, 9, 10, 11, 30, 60, 80, 100, 300, 1000, 10000).

4) **Exclude all responses from DNS forwarders that ever return a wrong answer:** We also excluded *all responses* from a DNS forwarder if it ever returned an incorrect IP address in a response for the query.

5) **Exclude all responses from caches in same country as domain name hosted:** For a given domain name, we excluded all DNS cache responses coming from DNS forwarders for ASNs in the same country where the domain name was *hosted*. For instance, if a domain name pointed to an IP address in Italy, we would exclude all DNS cache hits from Italy on that domain name as potential false positives.

6) **Exclude infrequent responses:** Unless resolvers in a given ASN returned at least four responses for a given domain that were not otherwise excluded, we excluded the responses for that domain from the ASN.

Our conditions for excluding results were very liberal, and could result in false negatives. Note that when we say we *excluded* a response, we mean that the response was not included as a final result. We continued to consider excluded responses as reasons to exclude other responses.

Why Is a Domain Name in the Cache?

There are many reasons a domain name may be in a cache (assuming we did not accidentally put it there). We are only interested in cache entries that might arise from suspected infections. We briefly introduce our working model of how NSO's Pegasus spyware deployments operate, supported by evidence from a *staged shutdown* of NSO Group's infrastructure.

Our mental model of deployment of the Pegasus spyware is that most operators have two C&C servers to which most infections talk, and that the rest of their infrastructure comprises domains that are used in exploit links. After reports concerning the use of Pegasus spyware were published by Amnesty International and Citizen Lab on August 1, 2018, a *staged shutdown* of the Pegasus infrastructure was conducted over a period of several days. At first, the bulk of frontend domains appeared to be shut down, while a handful of *final domains* (usually two) remained active for each operator. We believe that these were the C&C servers and that the domains were kept online so that infected devices would have an opportunity to beacon back and receive instructions on new C&C servers with which they should communicate.

If a given operator had exactly two final domains, we assumed that these were C&C servers. If an operator had more than two final domains, we assumed that some subset of size 2 were the C&C servers. We did not identify any operator for which our DNS cache probing technique reported hits on different subsets of size 2 from the final domains. We then filtered our responses for ASNs which had hits on both hypothesized C&C domains and considered these to be *suspected infections*.

The Experiments

Once we had developed our technique for reducing false positives, we DNS cache probed for all domains we linked to NSO Group's infrastructure that were active

and matching our fingerprints. We queried domains at least once per their period of authoritative TTL. Because of the large number of domains and servers, and our desire to conserve bandwidth, we alternated which domains we were probing. Each domain name was probed for at least three 24-hour periods.

Possible Limitations

Factors such as the use of VPNs and satellite Internet connections may skew our geolocation results. Thus, the country mapping should serve as a guide for further investigation, rather than ironclad evidence of monitoring. Additionally, it is possible that unusual configurations of DNS forwarders (such as the use of consistent hashing to consult different resolvers for different domain names) could defeat our filtering techniques and introduce false positives.

We are not sure what percentage of all DNS queries are observable by our method and note that the percentage could vary greatly across different countries and ISPs. Therefore, it is possible that our technique has missed a significant number of infections and may have failed to measure certain countries or ISPs entirely. Importantly, operators that appear in our results to be operating in a single country may actually be operating in multiple countries. We did not conduct any DNS cache probing of IPs in Mainland China.

5. Conclusion

This report identifies 45 countries with suspected Pegasus spyware infections operated by at least 33 likely NSO customers. We determined this by performing *DNS cache probing* on domain names we extracted from command and control (C&C) servers matching a newly devised fingerprint for Pegasus. We grouped the C&C servers, with each group representing a single Pegasus operator (assumed to be an NSO customer) using a technique that we call *Athena*. The resulting global map of NSO Pegasus infections reveals several issues of urgent concern.

Known spyware abusers operating Pegasus

While some NSO customers may be using Pegasus spyware as part of ‘lawful’ criminal or national security investigations investigations, at least six countries

with significant Pegasus operations have a public history of abusing spyware to target civil society.

Three Pegasus operators appear to be operational in Mexico, despite the extensive evidence of abuses of Pegasus to target Mexican civil society uncovered by Citizen Lab and our partners in 2017. The findings of widespread targeting in Mexico led to international outcry and a criminal investigation. However, they do not appear to have resulted in the termination of all of the Pegasus operations in that country.

In 2016, Citizen Lab exposed the use of Pegasus to target Ahmed Mansoor, a UAE-based human rights defender. Despite this disclosure and resulting public outcry, it appears that a suspected UAE-based Pegasus deployment remains operational. Most recently, a Saudi Arabia-linked campaign appears to be continuing, despite a recent investigation linking it to the targeting of an Amnesty International staff member and a Saudi activist.

Bahrain, another country that may host a Pegasus operator, has a notorious history of abusing spyware to target civil society. Notably, the operator linked to Bahrain appears to be using domain names with political themes, which is highly concerning, given that country's history of abuses of surveillance technology. The Togo-linked operator also appears to be using politically-themed domains. Togo has a history of authoritarian rule and human rights abuses.

Widespread cross-border surveillance with Pegasus

Ten Pegasus operators appear to be conducting surveillance in multiple countries. While we have observed prior cases of cross-border targeting, this investigation suggests that cross-border targeting and/or monitoring is a relatively common practice. The scope of this activity suggests that government-exclusive spyware is widely used to conduct activities that may be illegal in the countries where the targets are located. For example, we have identified several possible Pegasus customers *not linked to the United States, but with infections in US IP space*. While some of these infections may reflect usage of out-of-country VPN or satellite Internet service by targets, it is possible that several countries may be actively violating United States law by penetrating devices located within the US.

Failures at due diligence, contribution to global cyber insecurity

The cases identified in this report raise serious doubts as to the depth and seriousness of NSO's due diligence and concern for human rights protections. They also suggest that the company has a significant number of customers that maintain active infections in other countries, likely violating those countries laws. The global market for government exclusive spyware continues to grow, and as it does, more governments and security services with histories of abuse will acquire this technology. The expanding user base of spyware like Pegasus will enable a growing number of authoritarian states to pry into into the digital lives of their own citizens, but also into phones and computers in pockets and purses around the globe.

Communications with NSO Group

On 14 September 2018, Citizen Lab Director Ron Deibert sent a letter to two NSO Group principals, Mr. Omri Lavrie and Mr. Shalev Hulio, notifying them of the details of this report, explaining that we had shared an embargoed copy with journalists and offering to publish in full any response they wished to communicate on the record.

On 14 September 2018, Mr. Hulio responded by email saying "we have suggested several times in the past to meet you and your colleagues, but, unfortunately, our requests have been ignored." The Citizen Lab Director and staff have no record of any such outreach. Moreover, the Citizen Lab does not believe that a private meeting with researchers is a proper substitute for responsible public communication on such a serious matter of public interest.

Mr. Hulio also claimed "Contrary to statements made by you, our product is licensed to government and law enforcement agencies for the sole purpose of investigating and preventing crime and terror. Our business is conducted in strict compliance with applicable export control laws." Citizen Lab research does not speak to what statements NSO may make during marketing, sales, or export compliance. However, our research continues to demonstrate some highly concerning real-world examples of the abuse of NSO Group technology *in practice*. These uses have included apparent government customers of NSO Group abusing Pegasus spyware to target civil society groups, human rights defenders, lawyers, politicians, and journalists.

On 17 September 2018, we then received a public statement from NSO Group. The statement mentions that *"the list of countries in which NSO is alleged to operate is simply inaccurate. NSO does not operate in many of the countries listed."* This statement is a misunderstanding of our investigation: the list in our report is of suspected locations of NSO infections, it is not a list of suspected NSO customers. As we describe in **Section 3**, we observed DNS cache hits from what appear to be 33 distinct operators, some of whom appeared to be conducting operations in multiple countries. Thus, our list of 45 countries necessarily includes countries that are not NSO Group customers. We describe additional limitations of our method in **Section 4**, including factors such as VPNs and satellite connections, which can cause targets to appear in other countries.

The NSO statement also claims the "NSO's Business Ethics Committee, which includes outside experts from various disciplines, including law and foreign relations, reviews and approves each transaction and is authorized to reject agreements or cancel existing agreements where there is a case of improper use." We have seen no public details concerning the membership or deliberations of this committee but encourage NSO Group to disclose them. NSO's statements about a Business Ethics Committee recall the example of Hacking Team's "outside panel of technical experts and legal advisors … that reviews potential sales." This "outside panel" appears to have been a single law firm, whose recommendations Hacking Team did not always follow.

The continued supply of services to countries with problematic human rights track records and where highly-publicized abuses of spyware have occurred raise serious doubts about the effectiveness of this internal mechanism, if it exists at all.

Update

On 18 September 2018, NSO emailed the following addendum to their previous public statement:

"There are multiple problems with Citizen Lab's latest report. Most significantly, the list of countries in which NSO is alleged to sell or where our customers presumably operate the products is simply inaccurate. NSO does not sell its products in many of the countries listed. The product is only licensed to operate in countries approved under our Business Ethics Framework and the product will not operate outside of approved countries. As an example, the product is specifically designed to not operate in the USA."

In addition to our DNS cache probing technique showing suspected infections in the United States, we previously observed a suspected Mexican operator target a minor child in the United States with Pegasus infection attempts, including messages impersonating the US embassy. Also, as part of our *Million Dollar Dissident* report in 2016, we successfully infected our test phone (in the United States at the time) with a Pegasus link sent to UAE activist Ahmed Mansoor

Appendix A: Interesting Domains and ASNs of DNS Cache Hits by Operator

In this appendix we list DNS cache hits by ASN for all systems in which we observed them. We list some domain names for systems which may be used for political targeting, but redact domain names in other cases, as other systems may be used for legitimate law enforcement purposes.

Operator RECKLESS-1

Interesting Domains	Why interesting
universopolitico[.]net	May show political focus.
animal-politico[.]com	
un0noticias[.]com	Uno TV is a Mexican provider of news. The domain name **unonoticias[.]net** was previously used to target Mexican journalists with Pegasus spyware.
un0noticias[.]net	

Table 1: Interesting domains for operator RECKLESS-1.

Operator RECKLESS-2

Interesting Domains	Why interesting
noticiaspoliticos[.]com	May show political focus.
politicoportales[.]org	

Table 2: Interesting domains for operator RECKLESS-2.

Operator MAYBERECKLESS

ASN	Description	Country
8151	Uninet S.A. de C.V.	Mexico
13999	Mega Cable, S.A. de C.V.	Mexico
17072	TOTAL PLAY TELECOMUNICACIONES SA DE CV	Mexico
6503	Axtel, S.A.B. de C.V.	Mexico
18734	Operbes, S.A. de C.V.	Mexico

Table 3: Suspected infections for operator MAYBERECKLESS.

Operator PRICKLYPEAR

ASN	Description	Country
8151	Uninet S.A. de C.V.	Mexico
11888	Television Internacional, S.A. de C.V.	Mexico
17072	TOTAL PLAY TELECOMUNICACIONES SA DE CV	Mexico
13999	Mega Cable, S.A. de C.V.	Mexico
6503	Axtel, S.A.B. de C.V.	Mexico
28548	Cablevisión, S.A. de C.V.	Mexico
11172	Alestra, S. de R.L. de C.V.	Mexico
22773	Cox Communications Inc.	USA (Arizona)
7922	Comcast Cable Communications, LLC	USA (Arizona)

Table 4: Suspected infections for operator PRICKLYPEAR.

Operator AGUILAREAL

ASN	Description	Country
8151	Uninet S.A. de C.V.	Mexico
6503	Axtel, S.A.B. de C.V.	Mexico
17072	TOTAL PLAY TELECOMUNICACIONES SA DE CV	Mexico

Table 5: Suspected infections for operator AGUILAREAL.

Operator ORZELBIALY

ASN	Description	Country
8374	Polkomtel Sp. z o.o.	Poland
50767	FIBERLINK Sp. z o.o.	Poland
5617	Orange Polska Spolka Akcyjna	Poland
12912	T-mobile Polska Spolka Akcyjna	Poland
198112	PROSAT s.c.	Poland
29314	Vectra S.A.	Poland
12741	Netia SA	Poland

Table 6: Suspected infections for operator ORZELBIALY.

Operator EDELWEISS

ASN	Description	Country
3303	Swisscom (Switzerland) Ltd	Switzerland

Table 7: Suspected infections for operator EDELWEISS.

Operator 5LATS

ASN	Description	Country
12578	SIA Lattelecom	Latvia

Table 8: Suspected infections for operator 5LATS.

Operator REDLIONS

ASN	Description	Country
24691	TogoTelecom, Togo	Togo

Table 9: Suspected infections for operator REDLIONS.

Interesting Domains	Why interesting
politiques-infos[.]info	May show political focus.
nouveau-president[.]com	

Table 10: Interesting domains for operator REDLIONS.

Operator ATLAS

ASN	Description	Country
6713	Itissalat Al-MAGHRIB	Morocco
37705	Topnet	Tunisia
36947	Telecom Algeria	Algeria
3215	Orange	France
36925	Orange Maroc	Morocco
8220	COLT Technology Services Group Limited	France
5410	Bouygues Telecom SA	France
2609	Tunisia BackBone AS	Tunisia

ASN	Description	Country
15557	SFR SA	France
29571	Orange Cote D'ivoire	Cote D'ivoire
5384	Emirates Telecommunications Corporation	UAE

Table 11: Suspected infections for operator ATLAS.

Interesting Domains	Why interesting
revolution-news[.]co	May indicate political themes in targeting.

Table 12: Interesting domains for operator ATLAS.

Operator GRANDLACS

ASN	Description	Country
20294	MTN-	Uganda
29975	VODACOM-	South Africa
2905	TICSA-ASN	South Africa
5713	SAIX-NET	South Africa
37061	Safaricom	Kenya
36890	MTNRW-ASN	Rwanda
37228	Olleh-Rwanda-Networks	Rwanda
37027	SIMBANET-AS	Kenya

Table 13: Suspected infections for operator GRANDLACS.

Interesting Domains	Why interesting
politicalpress[.]org	May indicate political themes in targeting.

Table 14: Interesting domains for operator GRANDLACS.

Operator MULUNGUSHI

ASN	Description	Country
36962	MTN Zambia	Zambia
3741	IS	South Africa

Table 15: Suspected infections for operator MULUNGUSHI.

Operator FALCON

ASN	Description	Country
5384	Emirates Telecommunications Corporation	UAE
15802	Emirates Integrated Telecommunications Company PJSC (EITC-DU)	UAE

Table 16: Suspected infections for operator FALCON.

Interesting Domains	Why interesting
nomorewarnow[.]com	May indicate anti-war themes in the targeting; UAE is currently engaged in military operations in Yemen.

Table 17: Interesting domains for operator FALCON.

Operator BABYFALCON

ASN	Description	Country
5384	Emirates Telecommunications Corporation	UAE
15802	Emirates Integrated Telecommunications Company PJSC (EITC-DU)	UAE

Table 18: Suspected infections for operator BABYFALCON.

Operator MAYBEFALCON

ASN	Description	Country
5384	Emirates Telecommunications Corporation	UAE

Table 19: Suspected infections for operator MAYBEFALCON.

Operator PEARL

ASN	Description	Country
51375	VIVA Bahrain BSC Closed	Bahrain
5416	Bahrain Telecommunications Company (BATELCO) B.S.C.	Bahrain
39015	Mena Broadband Services WLL	Bahrain
8781	Ooredoo Q.S.C.	Qatar

Table 20: Suspected infections for operator PEARL.

Interesting Domains	Why interesting
14-tracking[.]com	May be a reference to the 2011 Bahrain protests, which started on Feb 14. The February 14 Youth Coalition is an ongoing presence in anti-government demonstrations.
shia-voice[.]com	May indicate targeting of the Shia community, a community targeted for political persecution by the Bahraini Government.

Table 21: Interesting domains for operator PEARL.

Operator KINGDOM

ASN	Description	Country
8781	Ooredoo Q.S.C.	Qatar
43766	MTC KSA	Saudi Arabia
25019	Saudi Telecom Company JSC	Saudi Arabia
35819	Bayanat Al-Oula For Network Services	Saudi Arabia
48832	Linkdotnet-Jordan	Jordan
8376	Jordan Data Communications Company LLC	Jordan
24863	LINKdotNET	Egypt
8452	TE-AS	Egypt
24835	RAYA Telecom – Egypt	Egypt
9051	IncoNet Data Management sal	Lebanon
42003	Libantelecom	Lebanon
6713	Itissalat Al-MAGHRIB	Morocco
2856	British Telecommunications PLC	UK
5769	Videotron Telecom Ltee	Canada (Quebec)
376	Reseau d’informations scientifiques du Quebec (RISQ)	Canada (Quebec)
9121	Turk Telekom	Turkey
203217	Horizon Scope Mobile Telecom WLL	Iraq
50597	ScopeSky Communication and Internet Ltd.	Iraq
3215	Orange	France
5416	Bahrain Telecommunications Company (BATELCO) B.S.C.	Bahrain
51375	VIVA Bahrain BSC Closed	Bahrain

Table 22: Suspected infections for operator KINGDOM.

Interesting Domains	Why interesting
social-life[.]info	Amnesty observed this targeted at a Saudi activist abroad. Another target possibly in Qatar; the Qatar link went viral on WhatsApp and Twitter.
akhbar-arabia[.]com	Targeted at an Amnesty Researcher.

Table 23: Interesting domains for operator KINGDOM.

Operator MIDDLE

ASN	Description	Country
42003	Libantelecom	Lebanon
8781	Ooredoo Q.S.C.	Qatar
8529	Oman Telecommunications Company (S.A.O.G)	Oman
50010	Omani Qatari Telecommunications Company SAOC	Oman
5384	Emirates Telecommunications Corporation	UAE
9121	Turk Telekom	Turkey
12670	Completel	France
48832	Linkdotnet-Jordan	Jordan
2609	Tunisia BackBone AS	Tunisia

Table 24: Suspected infections for operator MIDDLE.

Operator DOME

ASN	Description	Country
9121	Turk Telekom	Turkey
1680	013 NetVision Ltd	Israel
8551	Bezeq International	Israel
12849	Hot-Net internet services Ltd.	Israel
15975	Hadara	Palestine
12975	Palestine Telecommunications Company (PALTEL)	Palestine
51407	Mada ALArab LTD	Palestine
8781	Ooredoo Q.S.C.	Qatar
8737	KPN B.V.	Netherlands
7922	Comcast Cable Communications, LLC	USA (Southeast/Florida)

Table 25: Suspected infections for operator DOME.

Operator OLIVE-1

ASN	Description	Country
1680	013 NetVision Ltd	Israel

Table 26: Suspected infections for operator OLIVE-1.

Operator OLIVE-2

ASN	Description	Country
16116	Pelephone Communications Ltd.	Israel
1680	013 NetVision Ltd	Israel
9116	012 Smile Communications LTD.	Israel

Table 27: Suspected infections for operator OLIVE-2.

Operator OLIVE-3

ASN	Description	Country
16116	Pelephone Communications Ltd.	Israel
9116	012 Smile Communications LTD.	Israel

Table 28: Suspected infections for operator OLIVE-3.

Operator OLIVE-4

ASN	Description	Country
16116	Pelephone Communications Ltd.	Israel
8551	Bezeq International	Israel

Table 29: Suspected infections for operator OLIVE-4.

Operator BLACKBIRD

ASN	Description	Country
8781	Ooredoo Q.S.C.	Qatar
5089	Virgin Media Limited	UK
5607	Sky UK Limited	UK
6799	OTEnet S.A.	Greece
15802	Emirates Integrated Telecommunications Company PJSC (EITC-DU)	UAE
5384	Emirates Telecommunications Corporation	UAE
30873	Public Telecommunication Corporation	Yemen
9038	Batelco Jordan	Jordan
21003	GPTC Autonomous System, Tripoli Libya	Libya
21050	Fast Telecommunications Company W.L.L.	Kuwait
56478	Hyperoptic Ltd	UK
3225	Gulfnet Kuwait	Kuwait
20001	Time Warner Cable Internet LLC	USA (Southern California)

Table 30: Suspected infections for operator BLACKBIRD.

Operator CHANG

ASN	Description	Country
131090	CAT TELECOM Public Company Ltd,CAT	Thailand
7470	TRUE INTERNET Co.,Ltd.	Thailand
9931	The Communication Authoity of Thailand, CAT	Thailand

Table 31: Suspected infections for operator CHANG.

Operator GANGES

ASN	Description	Country
9498	BHARTI Airtel Ltd.	India
24560	Bharti Airtel Ltd., Telemedia Services	India
18209	Atria Convergence Technologies pvt ltd	India
17813	Mahanagar Telephone Nigam Limited	India
9829	National Internet Backbone	India
17488	Hathway IP Over Cable Internet	India
38571	Star Broadband Services	India
7738	Telemar Norte Leste S.A.	Brazil
45595	Pakistan Telecom Company Limited	Pakistan
45609	Bharti Airtel Ltd. AS for GPRS Service	India
4657	StarHub Internet Exchange	Singapore
45588	Bangladesh Telecommunications Company Limited (BTCL), Nationwide	Bangladesh

Table 32: Suspected infections for operator GANGES.

Interesting Domains	Why interesting
signpetition[.]co	May indicate political themes in the targeting.

Table 33: Interesting domains for operator GANGES.

Operator MERLION

ASN	Description	Country
4773	MobileOne Ltd. Mobile/ Internet Service Provider Singapore	Singapore
9506	Singtel Fibre Broadband	Singapore
10091	StarHub Cable Vision Ltd	Singapore

Table 34: Suspected infections for operator MERLION.

Operator SYRDARYA

ASN	Description	Country
8193	Uzbektelekom Joint Stock Company	Uzbekistan
34250	Uzbektelecom Joint-Stock Company	Uzbekistan
41750	Mega-Line Ltd.	Kyrgyzstan
8449	ElCat Ltd.	Kyrgyzstan
41329	SkyMobile LTD	Kyrgyzstan
29061	Saimanet Telecomunications	Kyrgyzstan
47139	Cjsc Indigo Tajikistan	Tajikistan
206026	Kar-Tel LLC	Kazakhstan
9121	Turk Telekom	Turkey
24722	LLC Babilon-T	Tajikistan
59668	PE Turon Media	Uzbekistan
12735	TurkNet Iletisim Hizmetleri A.S	Turkey
9198	JSC Kazakhtelecom	Kazakhstan
34718	LLC texnoprosistem	Uzbekistan
47452	Super iMAX	Uzbekistan
12365	Sarkor-Telecom	Uzbekistan
31203	Sharq Telekom CJSC	Uzbekistan
50025	Net Television Ltd	Uzbekistan

Table 35: Suspected infections for operator SYRDARYA.

Operator TULPAR

ASN	Description	Country
29555	Mobile Telecom-Service LLP	Kazakhstan
9198	JSC Kazakhtelecom	Kazakhstan

Table 36: Suspected infections for operator TULPAR.