Lookout®

Finding Wonderland Through the Rabbit Hole: Lookout's Mobile CTI

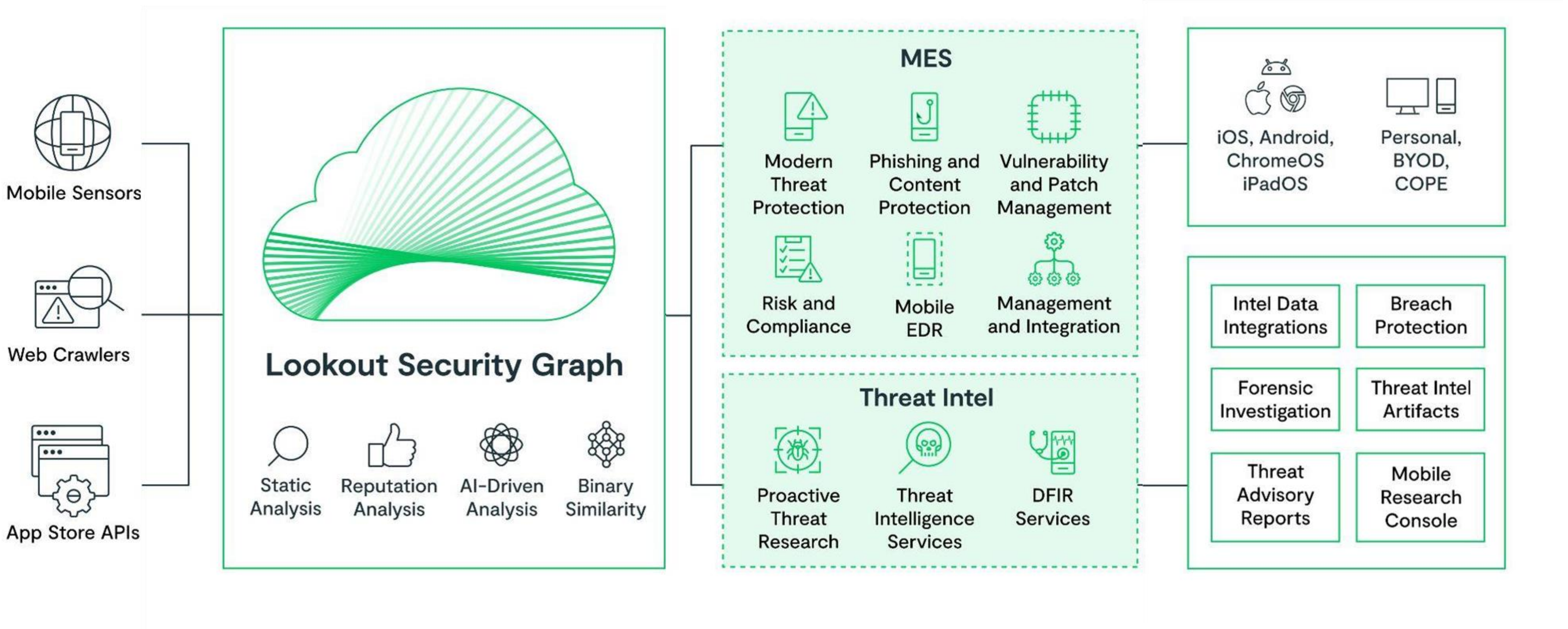
Where Our Data Comes From

220+ Million
Endpoint Devices

355+ Million
Apps Analyzed

464+ Million
Phishing and Malicious Sites

How Lookout Works



Lookout Security Graph

Acquisition

Mobile Network

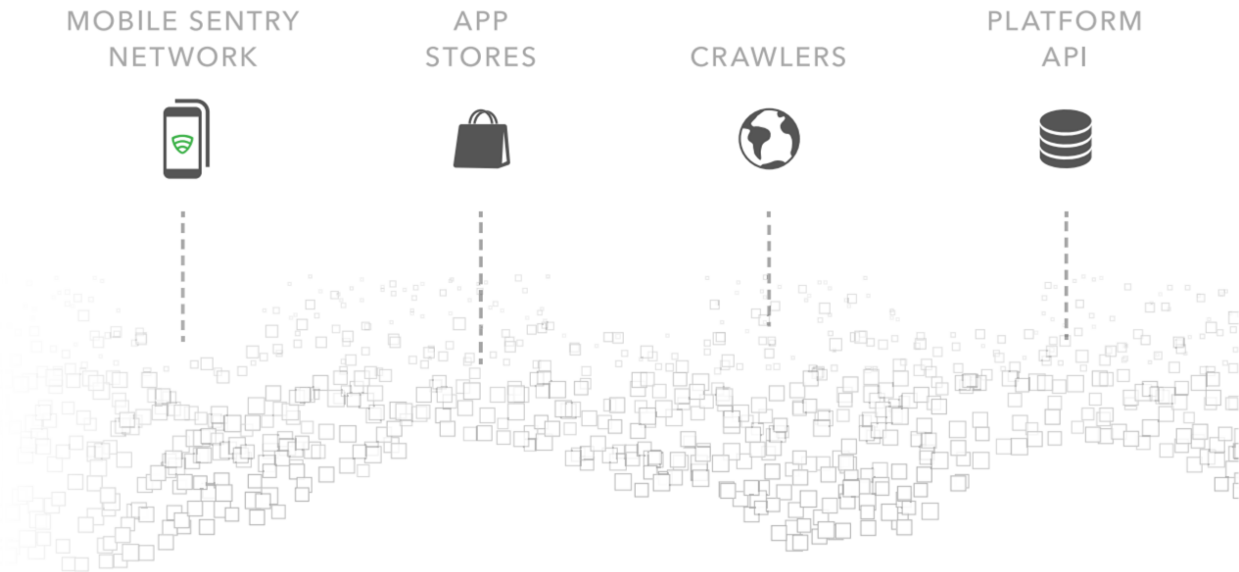
- More than 220 million devices worldwide provide a comprehensive, real-time view into global threats.
- Binary acquisition process shares the load among multiple devices to limit battery and data impact, later reassembling the app in the cloud.

Crawling

- Lookout monitors the major and minor app stores of the world, including popular app stores in countries such as China, Russia, and India.

APIs

- By serving as the security layer for many of the world's largest app stores, Lookout has privileged access to apps malware writers submit that never see the light of day.



Lookout Security Graph

Enrichment

Metadata

- Lookout appends data such as app name, digital signature, app store description, and developer name.

Reputation

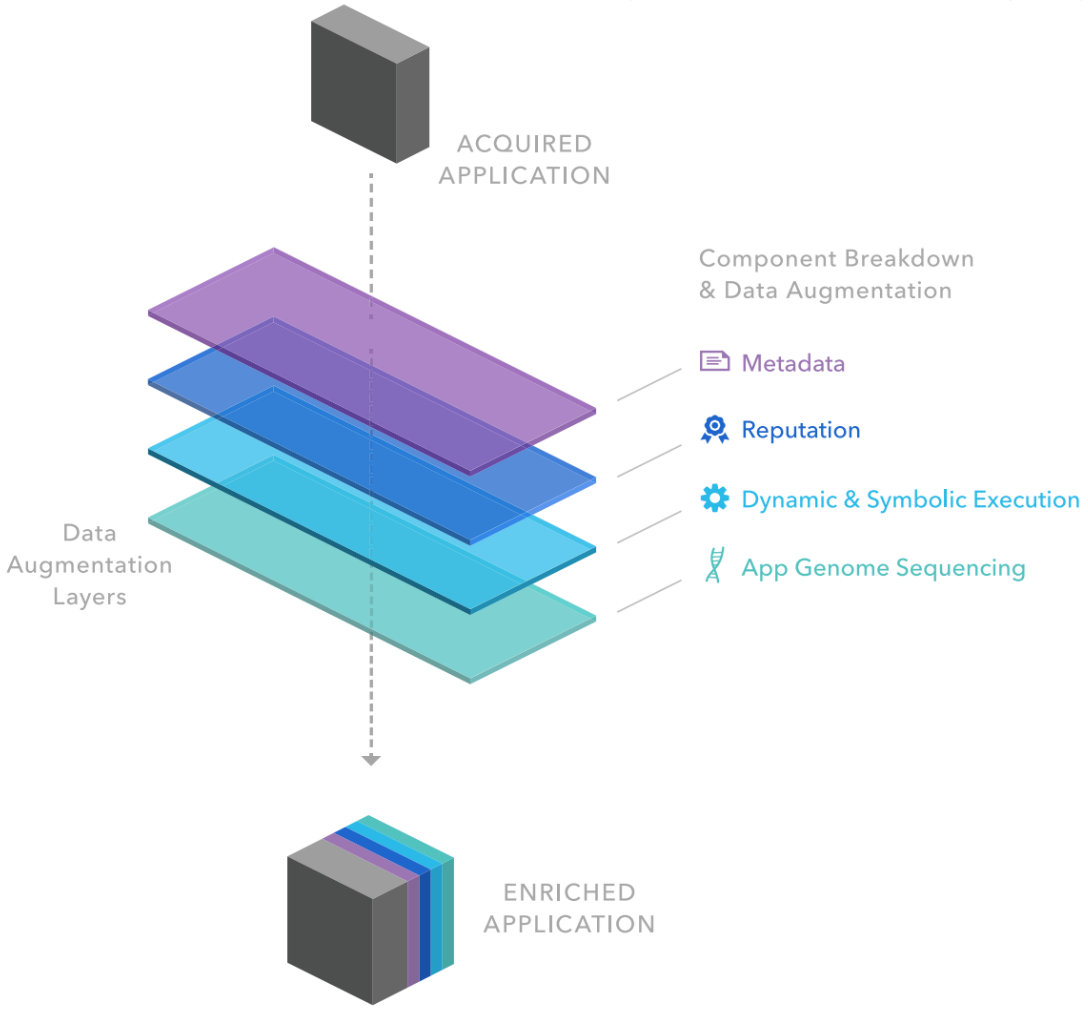
- Lookout incorporates data related to the authorship, origin, and geohistorical distribution of an app, such as the duration and location.

Behavior

- By serving as the security layer for many of the world's largest app stores, Lookout has privileged access to apps malware writers submit that never see the light of day.

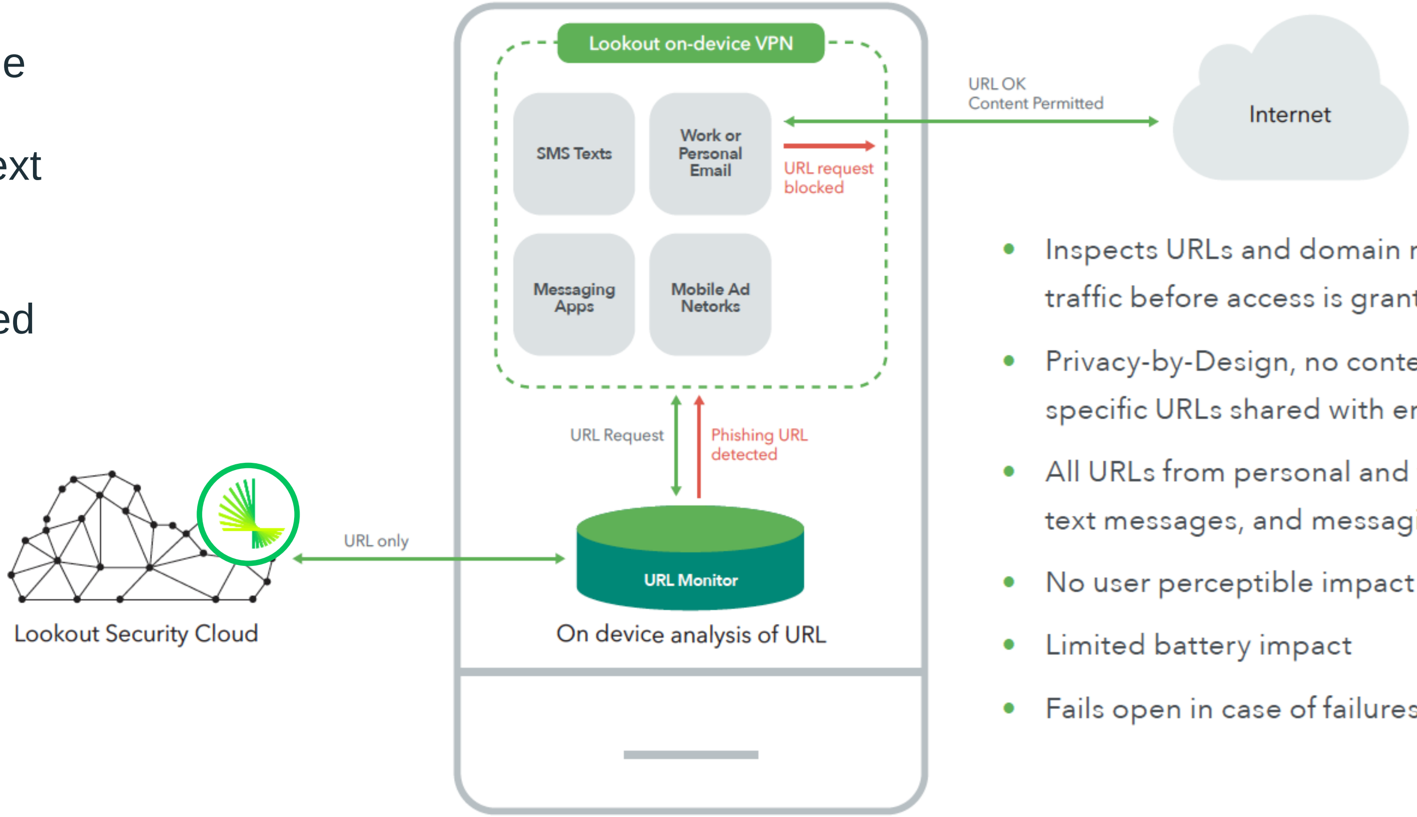
App Genome Sequencing

- The fuzzy code similarity the app shares with all code in the Lookout Security Graph reveals where that app's code (or its relatives) appear in the world.



Lookout Phishing and Content Protection

- Lookout PCP protects the whole device — including from applications and phishing via text message.
- Phishing attacks can be targeted specifically at mobile devices; Lookout coverage prioritizes phishing protection on mobile.



- Inspects URLs and domain names in network traffic before access is granted
- Privacy-by-Design, no content inspected, or specific URLs shared with enterprise admin
- All URLs from personal and work email apps, text messages, and messaging platforms
- No user perceptible impact on performance
- Limited battery impact
- Fails open in case of failures

The Cheshire Cat

Major Public Discoveries

2016-17

Pegasus
Remote surveillance

ViperRAT
Mobile RAT

Chrysaor
Remote root surveillance

SonicSpy
Targeted spyware

2018-19

DNC Phishing
Zero hour phishing attack

Dark Caracal
PC and Mobile APT

BeiTaAd
Malicious Adware

Monokle
Russian surveillanceware

2020

UN & NGO Phishing
Targeted campaign

Corona Live 1.1
App trojanized w/ Spymax

SilkBean
Chinese surveillanceware

Goontact
Mobile extortion campaign

2021

Hornbill & Sunbird
Surveillanceware and RAT

AbstractEmu
Rooting malware

BitScam & CloudScam
Android Crypto Scam

Anubis Distribution
Banking malware

2022

Hermit
Sophisticated Spyware

Moonshine
Chinese surveillanceware

Predatory Loan Apps
iOS and Android malware

2023

DragonEgg/WyrmSpy
Chinese Surveillanceware

BouldSpy
Iranian Surveillanceware

BadBazaar
Chinese Surveillanceware

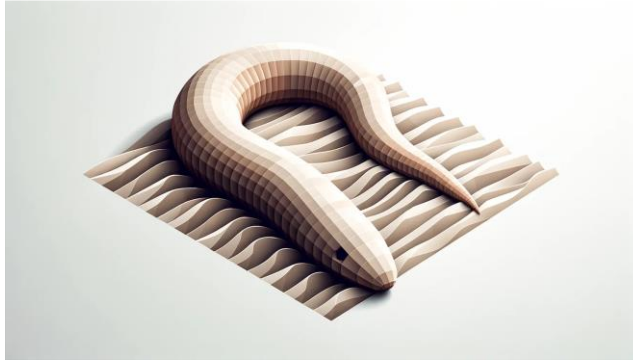
Infamous Chisel
Russian Surveillanceware

2024

CryptoChameleon
FCC & Crypto phishing

GuardZoo
Houthi-developed surveillanceware

Three Key Discoveries



Deblind

Attribution: Sandworm (RUS)

- Android spyware likely used to target the Ukranian military.
- One component of the Infamous Chisel Android surveillance tooling
- Sandworm APT is known to have connection to Russian intelligence organizations.

WyrmSpy & DragonEgg

Attribution: APT41 (CHN)

- Android surveillanceware developed by APT41.
- Tracked by Lookout and protected against since August 2017
- Sophisticated data collection and exfiltration capabilities. Can also download additional modules

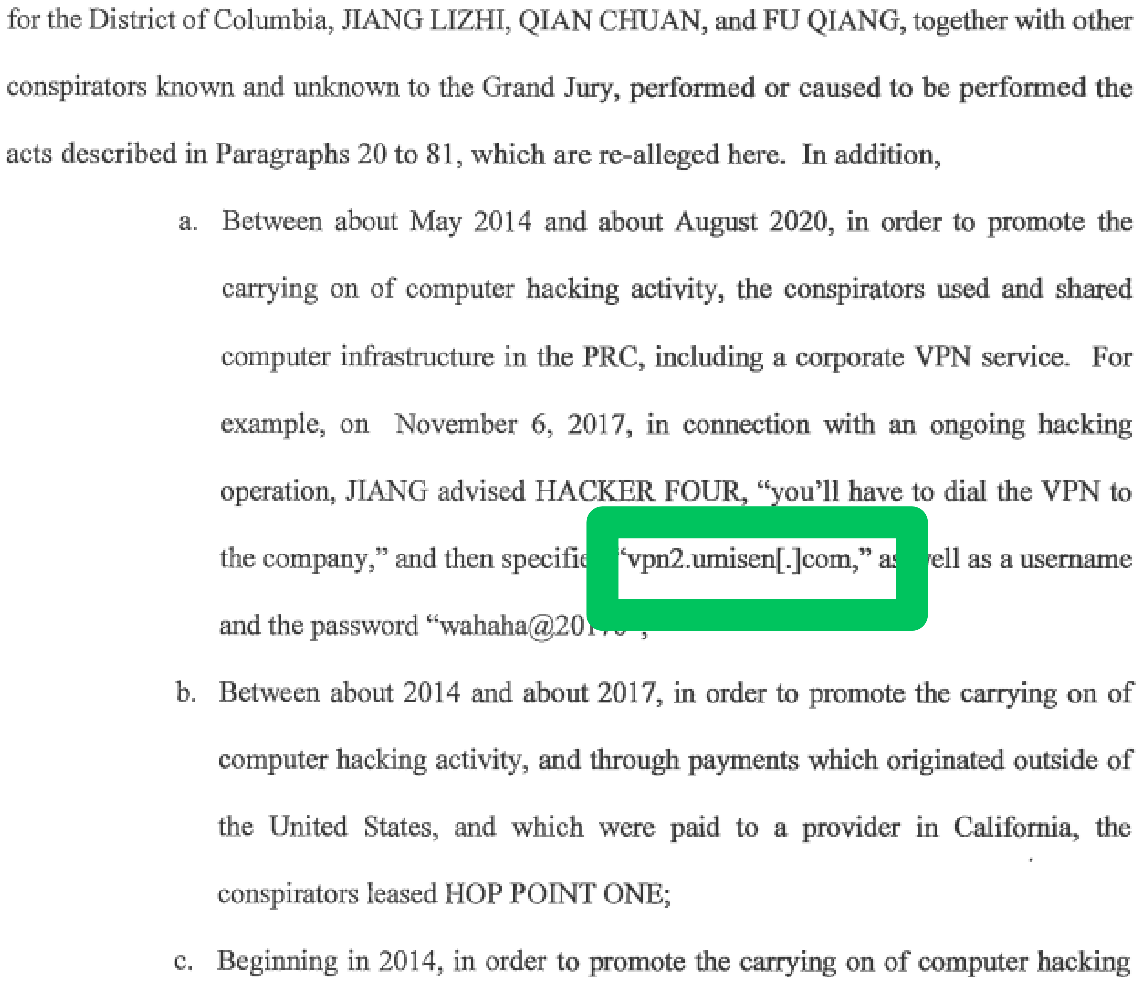
BadBazaar

Attribution: APT15 (CHN)

- iOS & Android surveillanceware targeting Tibetans and Uyghurs
- iOS variant was available on the App Store at one time.
- Extensive tracking and data collection capabilities that appear to be under continuous development.

All in the golden afternoon…

CHENGDU404 Indictment



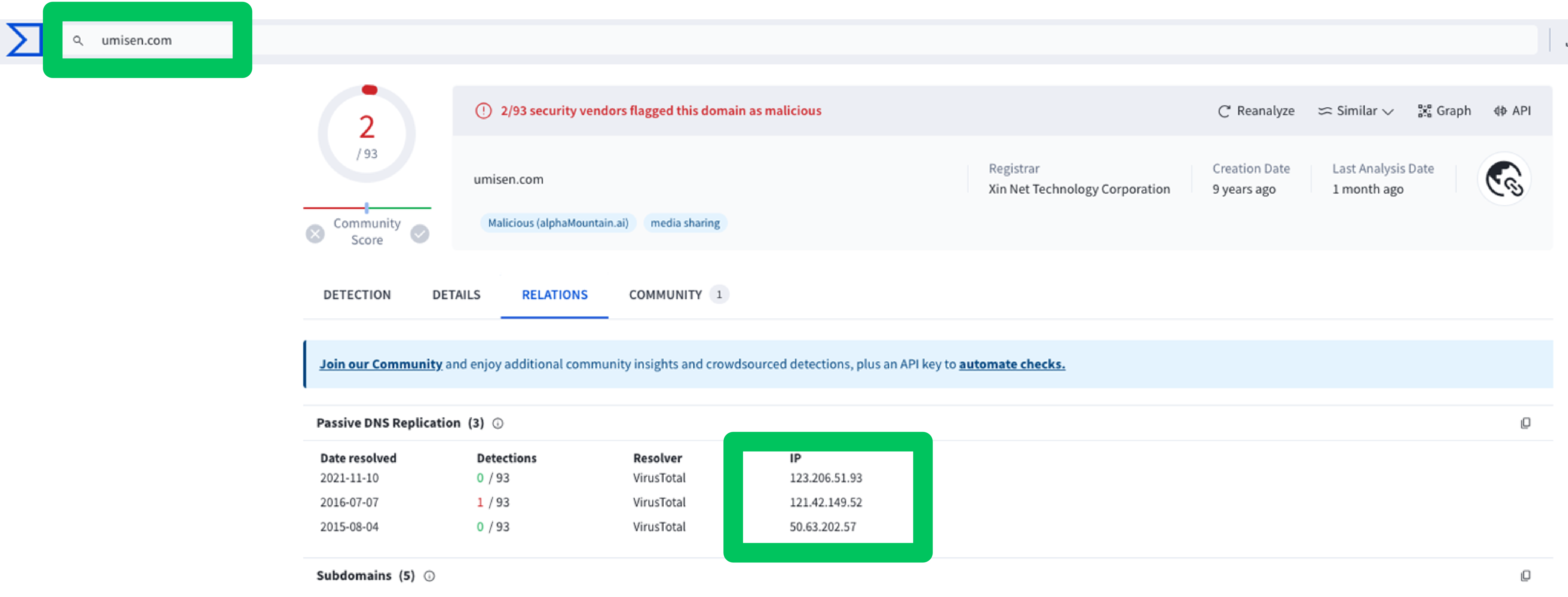
for the District of Columbia, JIANG LIZHI, QIAN CHUAN, and FU QIANG, together with other conspirators known and unknown to the Grand Jury, performed or caused to be performed the acts described in Paragraphs 20 to 81, which are re-alleged here. In addition,

a. Between about May 2014 and about August 2020, in order to promote the carrying on of computer hacking activity, the conspirators used and shared computer infrastructure in the PRC, including a corporate VPN service. For example, on November 6, 2017, in connection with an ongoing hacking operation, JIANG advised HACKER FOUR, "you'll have to dial the VPN to the company," and then specified "vpn2.umisen[.]com," as well as a username and the password "wahaha@20170";

b. Between about 2014 and about 2017, in order to promote the carrying on of computer hacking activity, and through payments which originated outside of the United States, and which were paid to a provider in California, the conspirators leased HOP POINT ONE;

c. Beginning in 2014, in order to promote the carrying on of computer hacking

Investigating Domain Information



umisen.com

2 / 93

Community Score

2/93 security vendors flagged this domain as malicious

umisen.com

Registrar	Creation Date	Last Analysis Date
Xin Net Technology Corporation	9 years ago	1 month ago

Malicious (alphaMountain.ai) media sharing

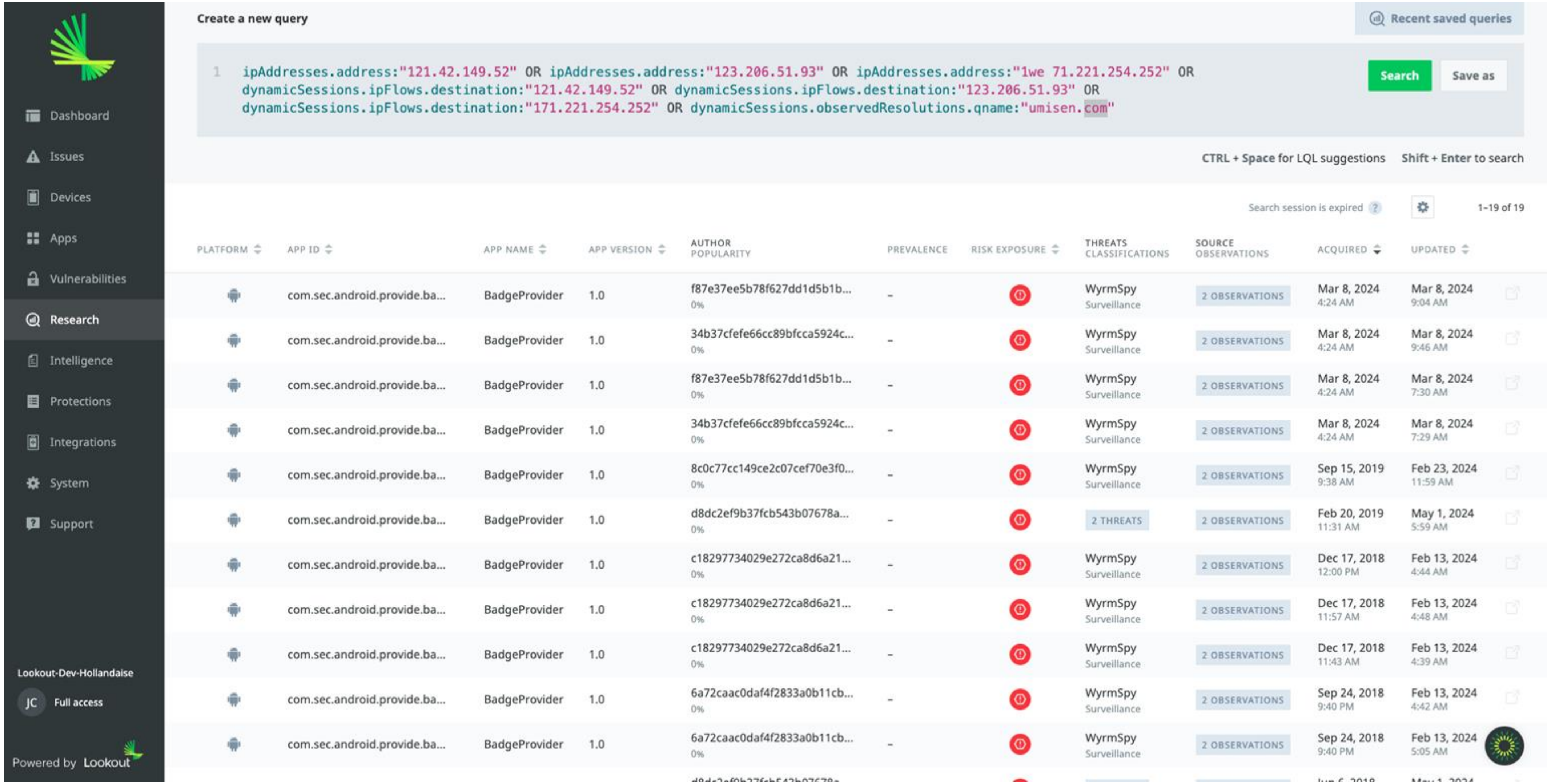
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Passive DNS Replication (3)

Date resolved	Detections	Resolver	IP
2021-11-10	0 / 93	VirusTotal	123.206.51.93
2016-07-07	1 / 93	VirusTotal	121.42.149.52
2015-08-04	0 / 93	VirusTotal	50.63.202.57

Subdomains (5)

Searching IP’s With Dynamic Analysis



Create a new query

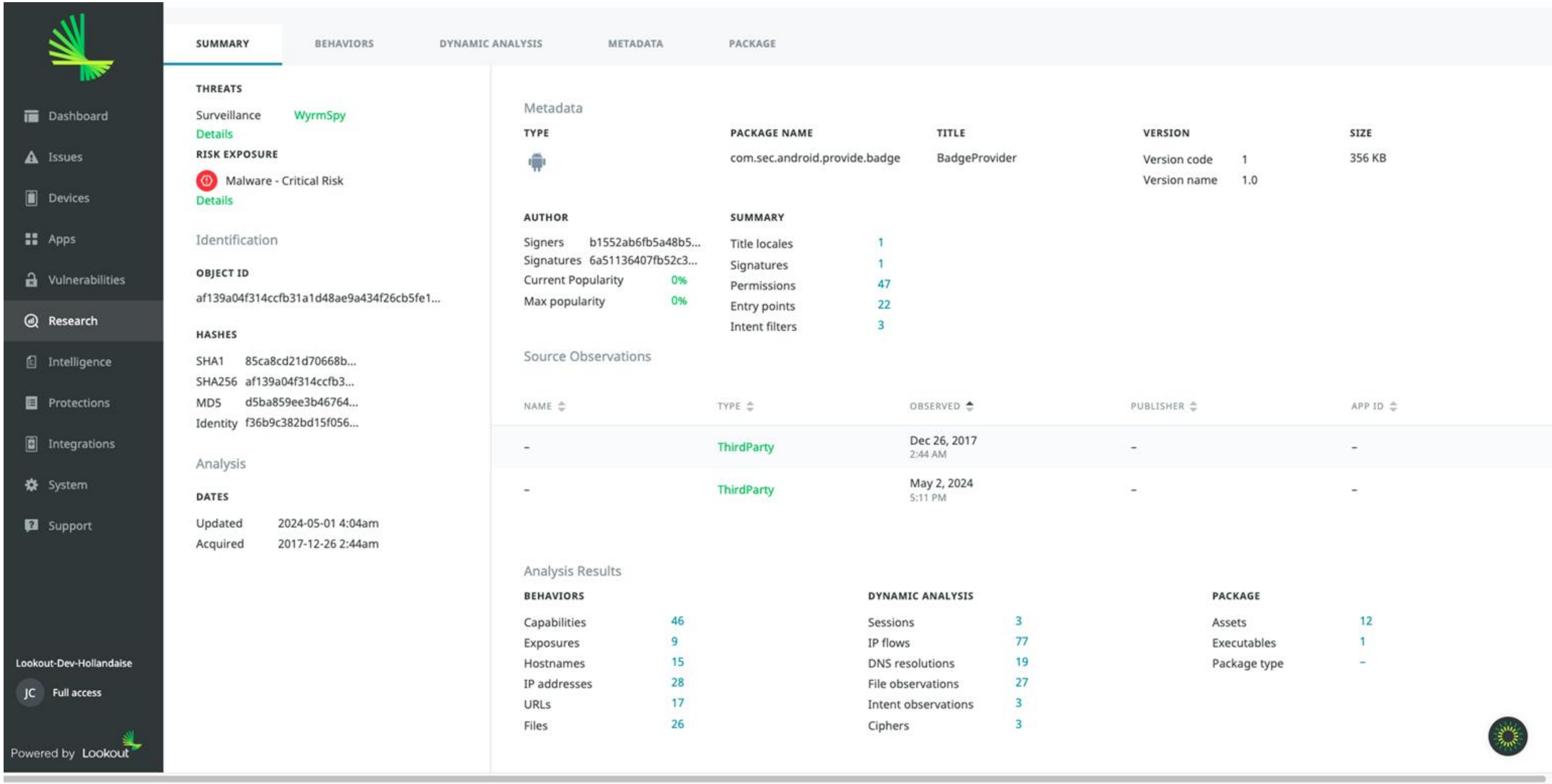
```
ipAddresses.address:"121.42.149.52" OR ipAddresses.address:"123.206.51.93" OR ipAddresses.address:"1we 71.221.254.252" OR
dynamicSessions.ipFlows.destination:"121.42.149.52" OR dynamicSessions.ipFlows.destination:"123.206.51.93" OR
dynamicSessions.ipFlows.destination:"171.221.254.252" OR dynamicSessions.observedResolutions.qname:"umisen.com"
```

CTRL + Space for LQL suggestions   Shift + Enter to search

Search session is expired ?   1-19 of 19

PLATFORM	APP ID	APP NAME	APP VERSION	AUTHOR POPULARITY	PREVALENCE	RISK EXPOSURE	THREATS CLASSIFICATIONS	SOURCE OBSERVATIONS	ACQUIRED	UPDATED
	com.sec.android.provide.ba...	BadgeProvider	1.0	f87e37ee5b78f627dd1d5b1b... 0%	-	●	WyrmSpy Surveillance	2 OBSERVATIONS	Mar 8, 2024 4:24 AM	Mar 8, 2024 9:04 AM
	com.sec.android.provide.ba...	BadgeProvider	1.0	34b37cfefe66cc89bfcca5924c... 0%	-	●	WyrmSpy Surveillance	2 OBSERVATIONS	Mar 8, 2024 4:24 AM	Mar 8, 2024 9:46 AM
	com.sec.android.provide.ba...	BadgeProvider	1.0	f87e37ee5b78f627dd1d5b1b... 0%	-	●	WyrmSpy Surveillance	2 OBSERVATIONS	Mar 8, 2024 4:24 AM	Mar 8, 2024 7:30 AM
	com.sec.android.provide.ba...	BadgeProvider	1.0	34b37cfefe66cc89bfcca5924c... 0%	-	●	WyrmSpy Surveillance	2 OBSERVATIONS	Mar 8, 2024 4:24 AM	Mar 8, 2024 7:29 AM
	com.sec.android.provide.ba...	BadgeProvider	1.0	8c0c77cc149ce2c07cef70e3f0... 0%	-	●	WyrmSpy Surveillance	2 OBSERVATIONS	Sep 15, 2019 9:38 AM	Feb 23, 2024 11:59 AM
	com.sec.android.provide.ba...	BadgeProvider	1.0	d8dc2ef9b37fcb543b07678a... 0%	-	●	2 THREATS	2 OBSERVATIONS	Feb 20, 2019 11:31 AM	May 1, 2024 5:59 AM
	com.sec.android.provide.ba...	BadgeProvider	1.0	c18297734029e272ca8d6a21... 0%	-	●	WyrmSpy Surveillance	2 OBSERVATIONS	Dec 17, 2018 12:00 PM	Feb 13, 2024 4:44 AM
	com.sec.android.provide.ba...	BadgeProvider	1.0	c18297734029e272ca8d6a21... 0%	-	●	WyrmSpy Surveillance	2 OBSERVATIONS	Dec 17, 2018 11:57 AM	Feb 13, 2024 4:48 AM
	com.sec.android.provide.ba...	BadgeProvider	1.0	c18297734029e272ca8d6a21... 0%	-	●	WyrmSpy Surveillance	2 OBSERVATIONS	Dec 17, 2018 11:43 AM	Feb 13, 2024 4:39 AM
	com.sec.android.provide.ba...	BadgeProvider	1.0	6a72caac0daf4f2833a0b11cb... 0%	-	●	WyrmSpy Surveillance	2 OBSERVATIONS	Sep 24, 2018 9:40 PM	Feb 13, 2024 4:42 AM
	com.sec.android.provide.ba...	BadgeProvider	1.0	6a72caac0daf4f2833a0b11cb... 0%	-	●	WyrmSpy Surveillance	2 OBSERVATIONS	Sep 24, 2018 9:40 PM	Feb 13, 2024 5:05 AM
				d8dc2ef9b37fcb543b07678a...					Jun 6, 2018	May 1, 2024

Investigating Malicious App



THREATS

Surveillance WyrmSpy
Details

RISK EXPOSURE

Malware - Critical Risk
Details

Identification

OBJECT ID

af139a04f314ccfb31a1d48ae9a434f26cb5fe1...

HASHES

SHA1	85ca8cd21d70668b...
SHA256	af139a04f314ccfb3...
MD5	d5ba859ee3b46764...
Identity	f36b9c382bd15f056...

Analysis

DATES

Updated	2024-05-01 4:04am
Acquired	2017-12-26 2:44am

Metadata

TYPE	PACKAGE NAME	TITLE	VERSION	SIZE
	com.sec.android.provide.badge	BadgeProvider	Version code 1 Version name 1.0	356 KB

AUTHOR

Signers	b1552ab6fb5a48b5...
Signatures	6a51136407fb52c3...
Current Popularity	0%
Max popularity	0%

SUMMARY

Title locales	1
Signatures	1
Permissions	47
Entry points	22
Intent filters	3

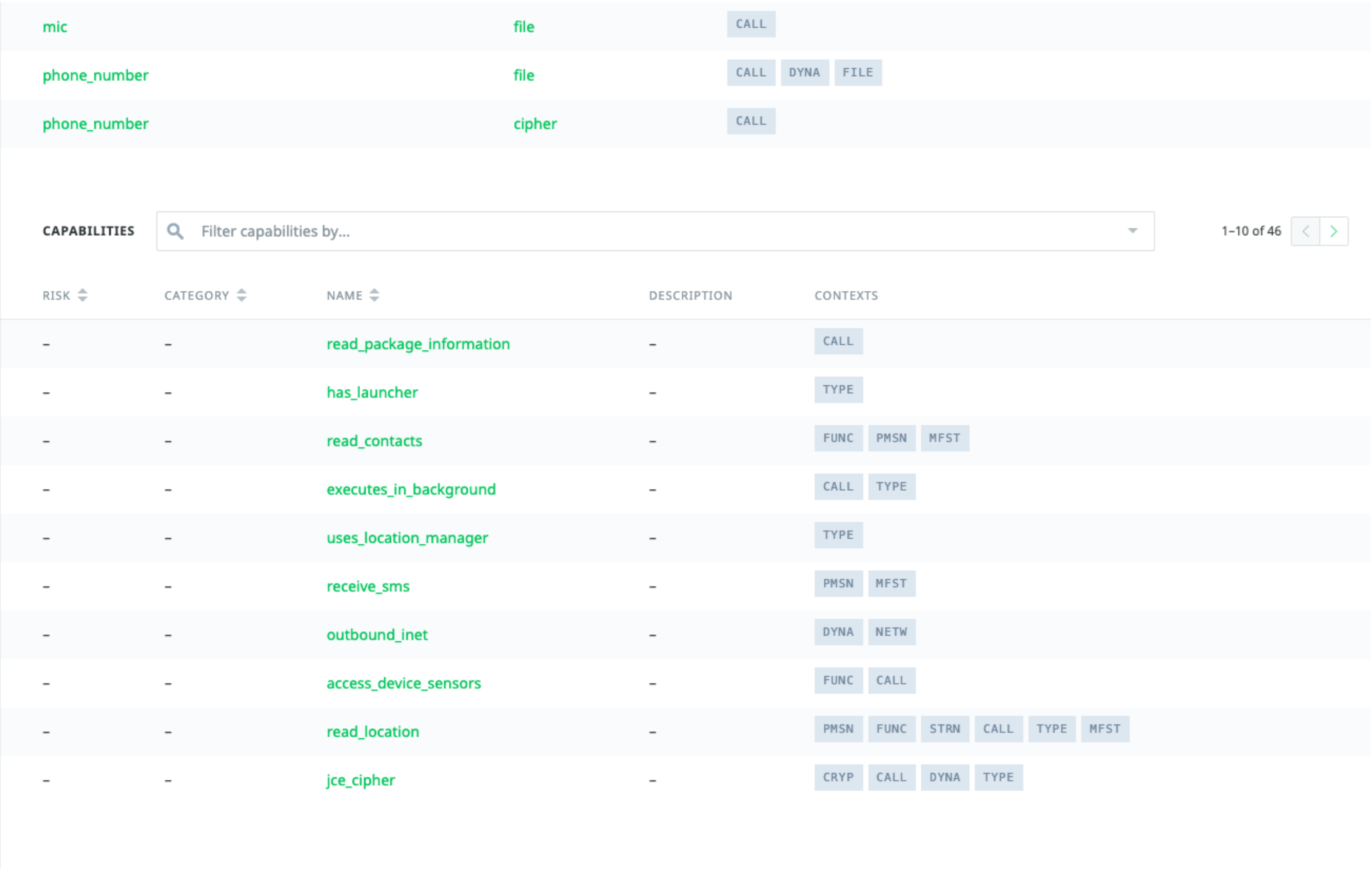
Source Observations

NAME	TYPE	OBSERVED	PUBLISHER	APP ID
-	ThirdParty	Dec 26, 2017 2:44 AM	-	-
-	ThirdParty	May 2, 2024 5:11 PM	-	-

Analysis Results

BEHAVIORS		DYNAMIC ANALYSIS		PACKAGE	
Capabilities	46	Sessions	3	Assets	12
Exposures	9	IP flows	77	Executables	1
Hostnames	15	DNS resolutions	19	Package type	-
IP addresses	28	File observations	27		
URLs	17	Intent observations	3		
Files	26	Ciphers	3		

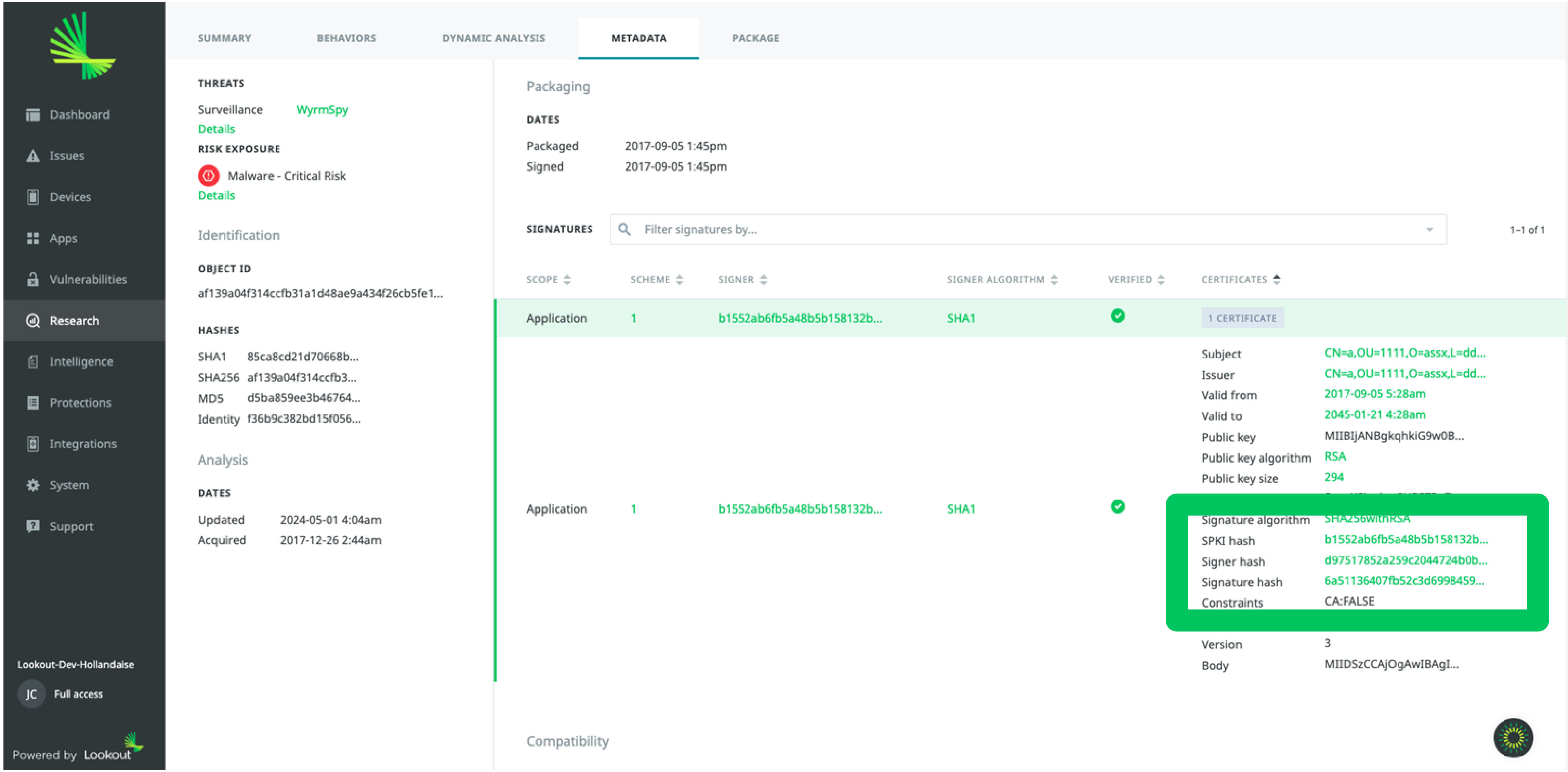
Understanding App Capabilities



mic	file	CALL
phone_number	file	CALL DYNA FILE
phone_number	cipher	CALL

RISK	CATEGORY	NAME	DESCRIPTION	CONTEXTS
–	–	read_package_information	–	CALL
–	–	has_launcher	–	TYPE
–	–	read_contacts	–	FUNC PMSN MFST
–	–	executes_in_background	–	CALL TYPE
–	–	uses_location_manager	–	TYPE
–	–	receive_sms	–	PMSN MFST
–	–	outbound_inet	–	DYNA NETW
–	–	access_device_sensors	–	FUNC CALL
–	–	read_location	–	PMSN FUNC STRN CALL TYPE MFST
–	–	jce_cipher	–	CRYP CALL DYNA TYPE

Pivoting Using Spooky Hash



THREATS

Surveillance WyrmSpy
Details

RISK EXPOSURE

Malware - Critical Risk
Details

Identification

OBJECT ID

af139a04f314ccfb31a1d48ae9a434f26cb5fe1...

HASHES

SHA1	85ca8cd21d70668b...
SHA256	af139a04f314ccfb3...
MD5	d5ba859ee3b46764...
Identity	f36b9c382bd15f056...

Analysis

DATES

Updated	2024-05-01 4:04am
Acquired	2017-12-26 2:44am

Packaging

DATES

Packaged	2017-09-05 1:45pm
Signed	2017-09-05 1:45pm

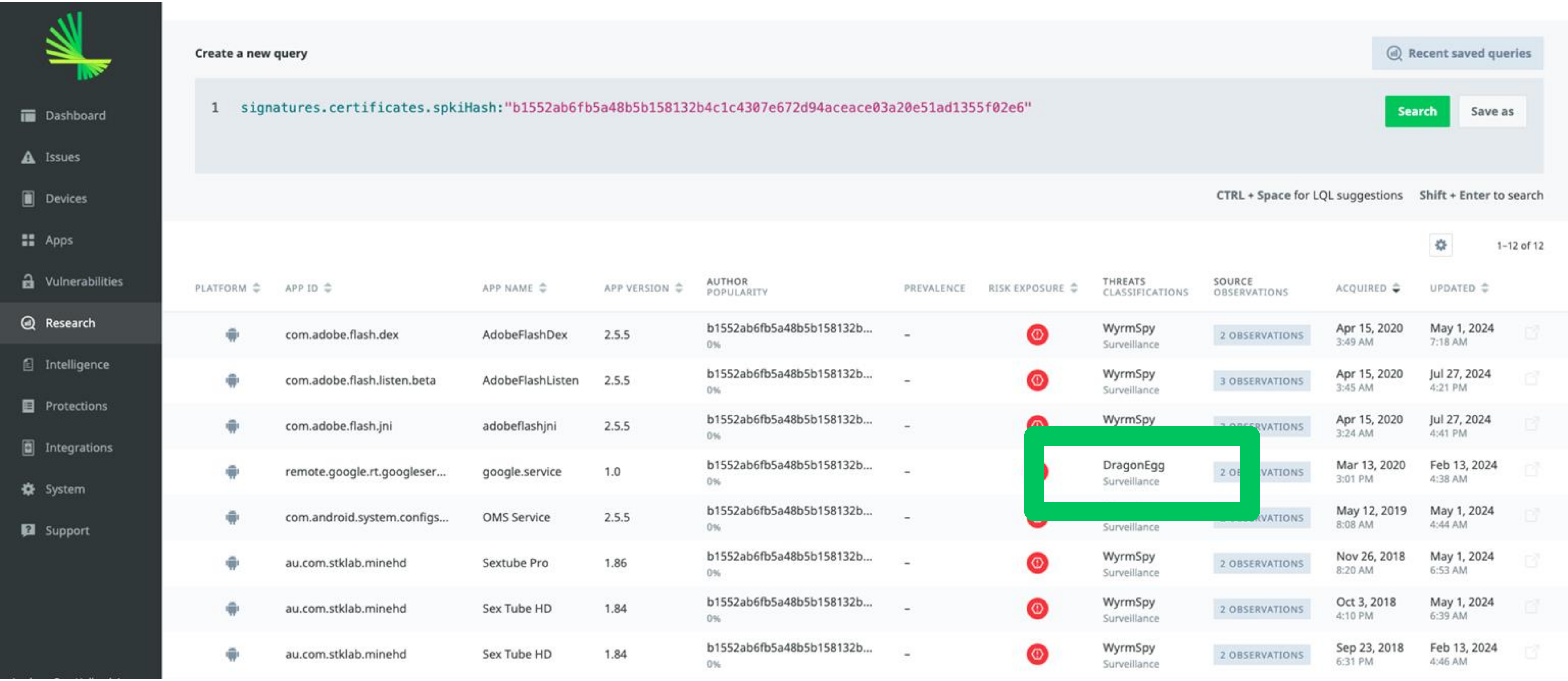
SIGNATURES Filter signatures by... 1–1 of 1

SCOPE	SCHEME	SIGNER	SIGNER ALGORITHM	VERIFIED	CERTIFICATES
Application	1	b1552ab6fb5a48b5b158132b...	SHA1	✓	1 CERTIFICATE
Application	1	b1552ab6fb5a48b5b158132b...	SHA1	✓	

Subject	CN=a,OU=1111,O=assx,L=dd...
Issuer	CN=a,OU=1111,O=assx,L=dd...
Valid from	2017-09-05 5:28am
Valid to	2045-01-21 4:28am
Public key	MIIBIjANBgkqhkiG9w0B...
Public key algorithm	RSA
Public key size	294
Signature algorithm	SHA256withRSA
SPKI hash	b1552ab6fb5a48b5b158132b...
Signer hash	d97517852a259c2044724b0b...
Signature hash	6a51136407fb52c3d6998459...
Constraints	CA:FALSE
Version	3
Body	MIIDSzCCAjOgAwIBAgI...

Compatibility

Reuse of Certs



Create a new query

```
signatures.certificates.spkiHash:"b1552ab6fb5a48b5b158132b4c1c4307e672d94aceace03a20e51ad1355f02e6"
```

CTRL + Space for LQL suggestions   Shift + Enter to search

1–12 of 12

PLATFORM	APP ID	APP NAME	APP VERSION	AUTHOR POPULARITY	PREVALENCE	RISK EXPOSURE	THREATS CLASSIFICATIONS	SOURCE OBSERVATIONS	ACQUIRED	UPDATED
	com.adobe.flash.dex	AdobeFlashDex	2.5.5	b1552ab6fb5a48b5b158132b... 0%	-	●	WyrmSpy Surveillance	2 OBSERVATIONS	Apr 15, 2020 3:49 AM	May 1, 2024 7:18 AM
	com.adobe.flash.listen.beta	AdobeFlashListen	2.5.5	b1552ab6fb5a48b5b158132b... 0%	-	●	WyrmSpy Surveillance	3 OBSERVATIONS	Apr 15, 2020 3:45 AM	Jul 27, 2024 4:21 PM
	com.adobe.flash.jni	adobeflashjni	2.5.5	b1552ab6fb5a48b5b158132b... 0%	-	●	WyrmSpy	[illegible] OBSERVATIONS	Apr 15, 2020 3:24 AM	Jul 27, 2024 4:41 PM
	remote.google.rt.googleser...	google.service	1.0	b1552ab6fb5a48b5b158132b... 0%	-	●	DragonEgg Surveillance	2 OBSERVATIONS	Mar 13, 2020 3:01 PM	Feb 13, 2024 4:38 AM
	com.android.system.configs...	OMS Service	2.5.5	b1552ab6fb5a48b5b158132b... 0%	-	●	[illegible] Surveillance	[illegible] OBSERVATIONS	May 12, 2019 8:08 AM	May 1, 2024 4:44 AM
	au.com.stklab.minehd	Sextube Pro	1.86	b1552ab6fb5a48b5b158132b... 0%	-	●	WyrmSpy Surveillance	2 OBSERVATIONS	Nov 26, 2018 8:20 AM	May 1, 2024 6:53 AM
	au.com.stklab.minehd	Sex Tube HD	1.84	b1552ab6fb5a48b5b158132b... 0%	-	●	WyrmSpy Surveillance	2 OBSERVATIONS	Oct 3, 2018 4:10 PM	May 1, 2024 6:39 AM
	au.com.stklab.minehd	Sex Tube HD	1.84	b1552ab6fb5a48b5b158132b... 0%	-	●	WyrmSpy Surveillance	2 OBSERVATIONS	Sep 23, 2018 6:31 PM	Feb 13, 2024 4:46 AM

Threat Actor Targeting Trends

- Exploits are the #1 initial access vector by leading incident response vendor reports. 52.8% of mobile devices ran on vulnerable OSs in 2023.

- Traditional EDR solutions are highly limited and less mature on mobile devices. Threat actors target mobile devices for this exact reason.

- 2023 saw the highest number of mobile attacks ever of 33.8 million. This marked a 50% increase from the previous year’s figures.

Lookout®

Thank You