Blockade.IO

One-click browser defense

Who Am I?

- VP of Product for RiskIQ
- Former analyst focused on automation
- Creator of various security tools
  - PassiveTotal (now with RiskIQ) - Analyst platform to research threats
  - HyperTotal - Virustotal submitter ID research
  - PDF X-RAY - Platform to analyze PDFs and collaborate
  - Various small scripts and other one-off tools
- Coffee roaster

Web Browsers

Everybody has one

- One of the most dynamic applications bundled with operating systems

Web Browsers

Everybody has one

- One of the most dynamic applications bundled with operating systems
- Used by all audiences from least technical to most technical

Web Browsers

Everybody has one

- One of the most dynamic applications bundled with operating systems
- Used by all audiences from least technical to most technical
- Increasingly becoming more and more powerful with new functionality

Web Browsers

Everybody has one

- One of the most dynamic applications bundled with operating systems
- Used by all audiences from least technical to most technical
- Increasingly becoming more and more powerful with new functionality
- **Act as a vehicle for most modern attacks**

Web Browsers Weaknesses

- Core technology stack and plug-ins
  - Exploitation of the browser, plug-ins or both pose issues
- Limited means to control where users go
  - Requires hosted DNS, network interception or local agents
- Serve as a vehicle for other attacks
  - Inbound links from email, shows user a web page or auto-exploits
  - Offer up downloads that may contain malicious exploits
- Difficult to understand what's loaded as you browse
  - Modern-day web pages make hundreds of requests to build a page
  - Websites can dynamically change based on headers, location, etc.
- They are ingrained in our everyday lives
  - We use web browsers so often, it's hard to maintain a level of vigilance

Attack Success

Impact is relative to the subject of the compromise

- Personal
  - User may have money stolen from bank accounts or lose personal information
  - Files could be encrypted and held for ransom
- Corporate
  - Attack may pivot further into the corporate network and steal company assets
- Civil Society
  - User may reveal sensitive contacts
  - Could result in detainment or worse

Attack Success

Impact is relative to the subject of the compromise

- Personal
  - User may have money stolen from bank accounts or lose personal information
  - Files could be encrypted and held for ransom
- Corporate
  - Attack may pivot further into the corporate network and steal company assets
- **Civil Society**
  - **User may reveal sensitive contacts**
  - **Could result in detainment or worse**

Who's worked with activists, journalists or NGOs?

Details to Consider

- Compromises have real-world impacts (arrests, physical attack, etc.)
  - Success may be getting location coordinates, gathering contacts or planting evidence in order to create a set of false charges for detainment
- Total attack surface could simply be one individual, not an organization
  - This may involve a physical component as well (i.e. send message when user leaves)
- General lack of funding, technology resources, time, subject matter expertise
  - Core focus is the mission - helping constituents
  - Education becomes a critical resource for defending against attacks

Initial Problem Case

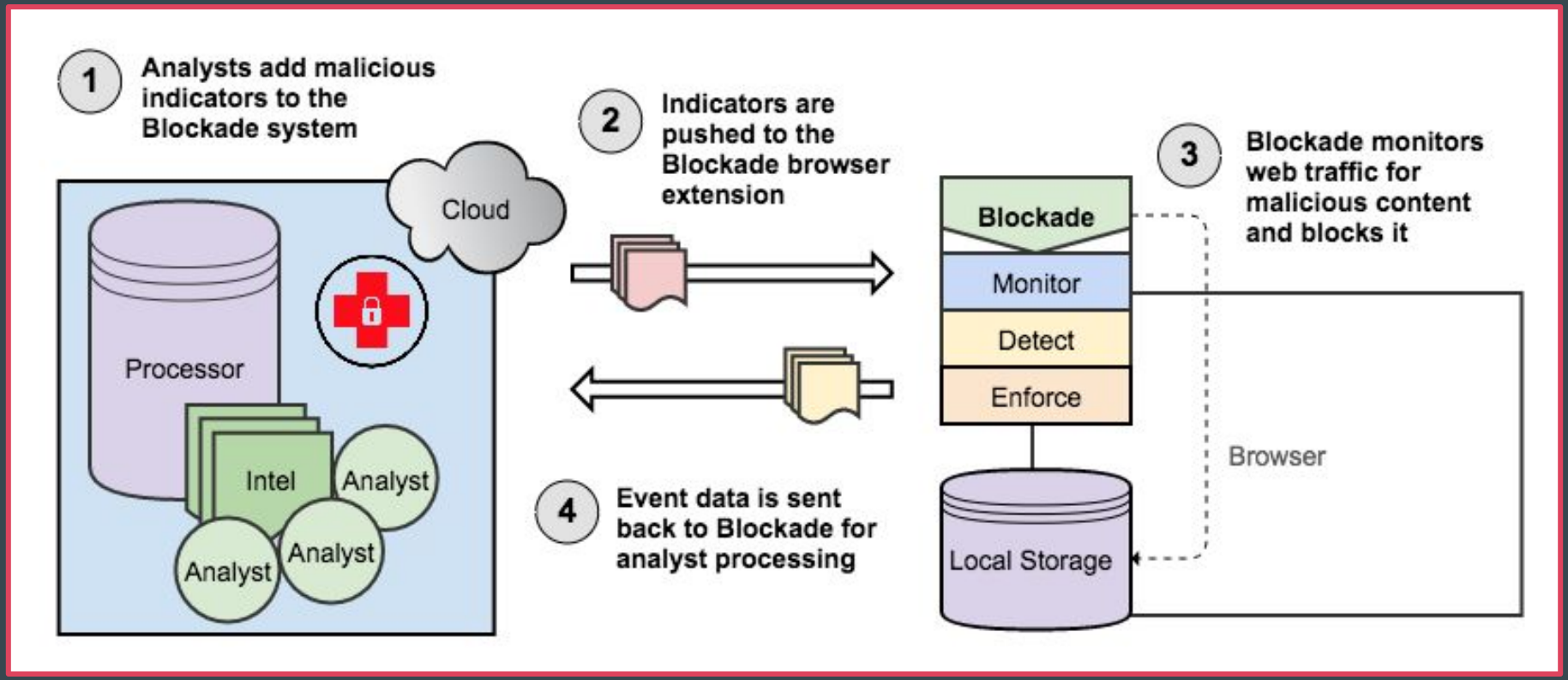
The Citizen Lab was observing a high-rate of phishing attempts against Tibetan groups from suspected Chinese state-sponsored actors. Email accounts were being compromised and stolen data was reused to target and exploit close contacts. Awareness needed to be raised across multiple non-profits without any central technology contacts.

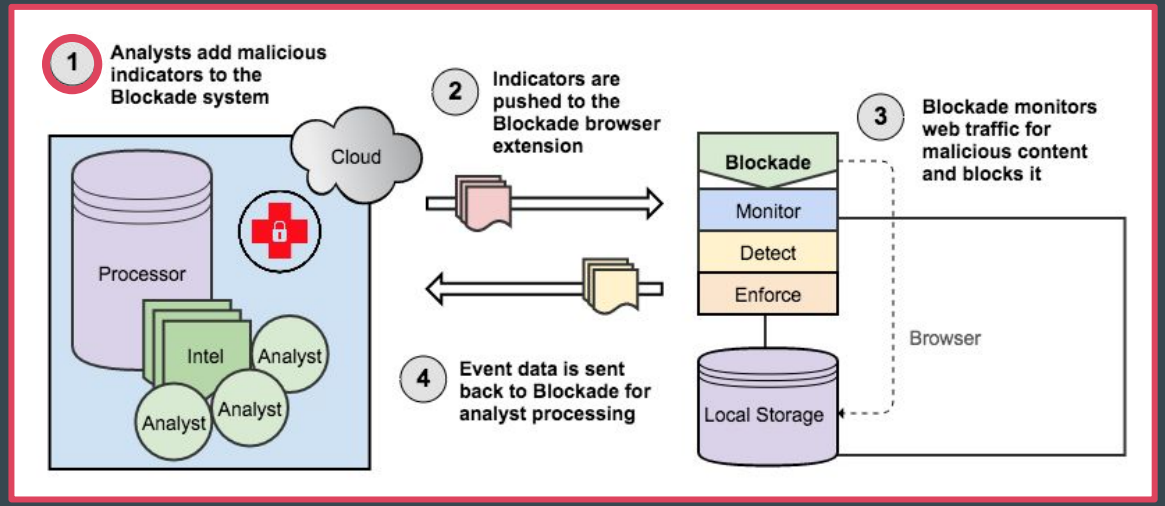
- Requirements for success
  - Solution needed to be cross-platform as much as possible
  - Solution needed to require little-to-no change in user behavior
  - Solution needed to scale with little money or technology
  - Solution needed to allow for collaboration
  - Solution needed to block specific resources deemed malicious
  - Solution needed to send data back to a central location
  - Solution needed to be open source

Several iterations later...

Blockade.IO : Suite for Browser Defense

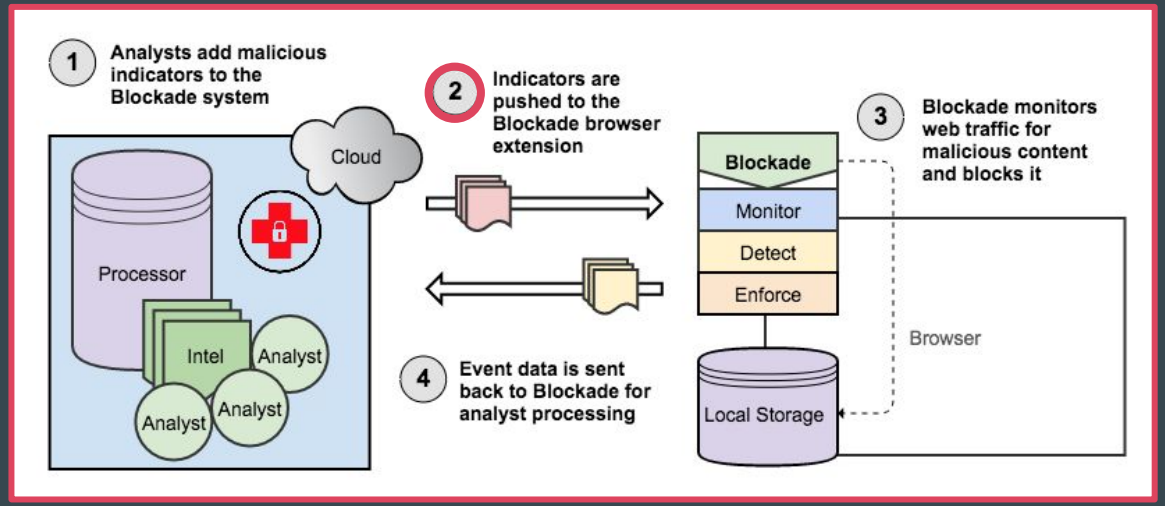
- **Browser Extension** that can install with one-click
  - Automatically updates, allows for federated nodes, capable of blocking threats
- **Cloud Node** that can run on micro VPS or via serverless infrastructure
  - Can be stood up within minutes using docker or code checkout
  - Offers administrator API and analyst APIs to manage indicators
- **Analyst Tool Bench** that can publish and interact with cloud nodes
  - Pre-hashes content sent to the cloud nodes to avoid data leaks
  - Built-in screening and checks so whitelisted items aren't blocked


1
Analysts add malicious indicators to the Blockade system
Cloud
Processor
Intel
Analyst
Analyst
Analyst
2
Indicators are pushed to the Blockade browser extension
3
Blockade monitors web traffic for malicious content and blocks it
Blockade
Monitor
Detect
Enforce
Browser
Local Storage
4
Event data is sent back to Blockade for analyst processing



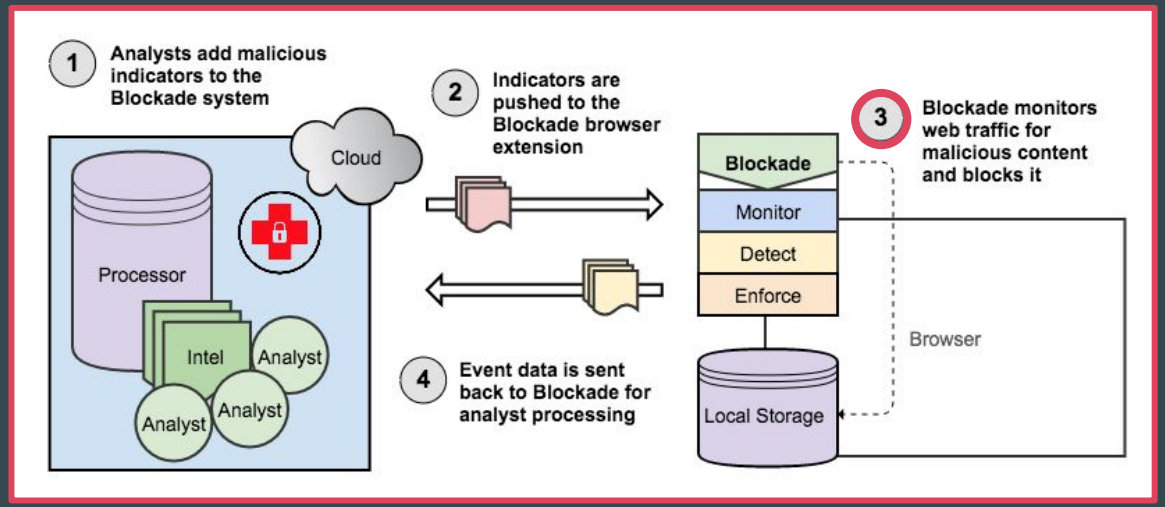
#1

- Cloud nodes are installed locally or users gain access to public instances
- Malicious and suspicious indicators are stored inside of the nodes
  - Analyst tool bench or admin API can be used to handle this
- Indicators can be hashed by users or will be hashed when processed
  - Avoids issues where someone doesn't want to share a sensitive indicator
  - No need for cloud nodes or extensions to understand the raw indicator



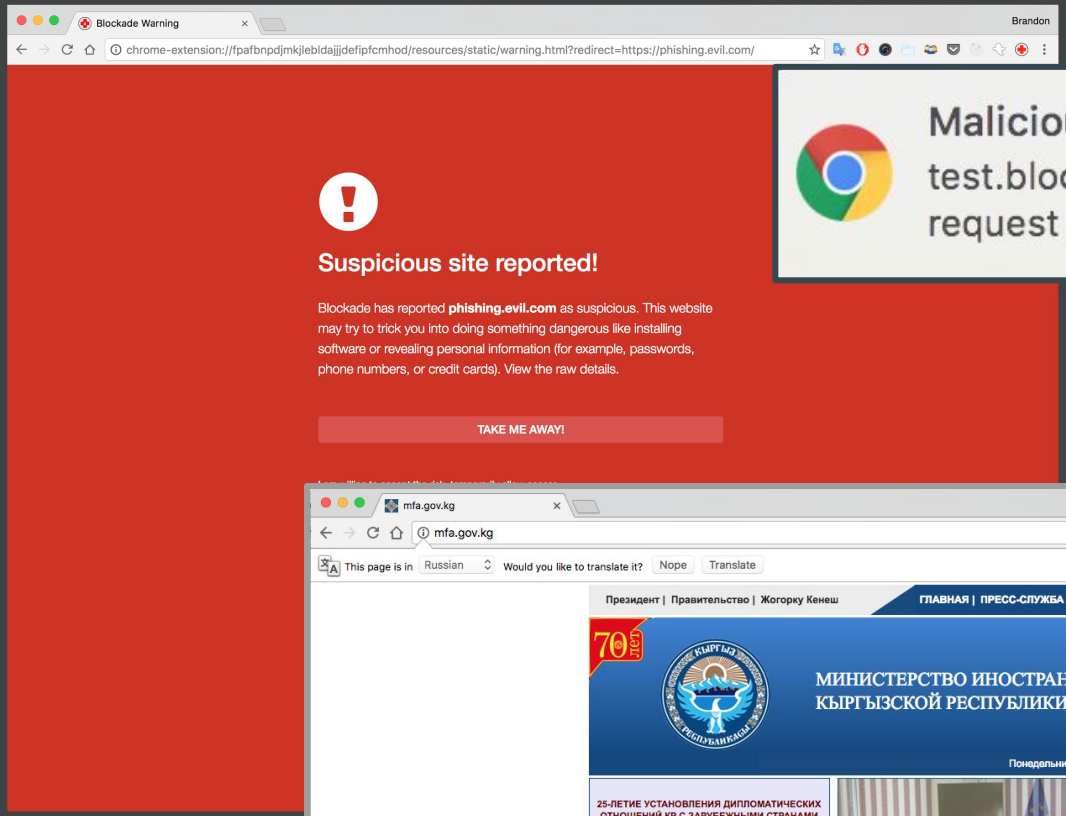
#2

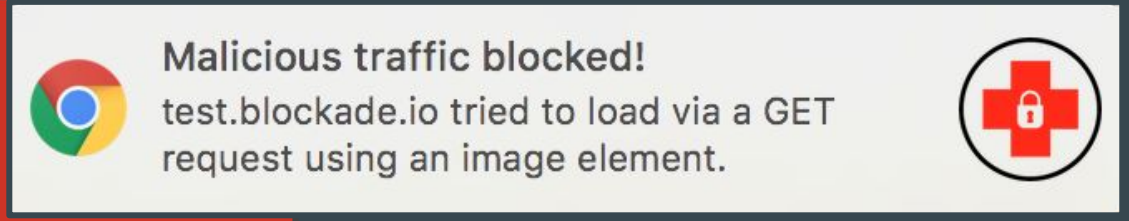
- Browser extension is installed within the user's web browser
  - Extensions come default configured to use public cloud nodes, but others can be added
  - Database sync is performed automatically
  - Deployment can be controlled through GPOs or master preferences
- Browsers get a copy of a hashed set of indicators
  - If small enough, data is stored within local storage
  - If too big, data is stored in memory (checks in place to keep in sync)

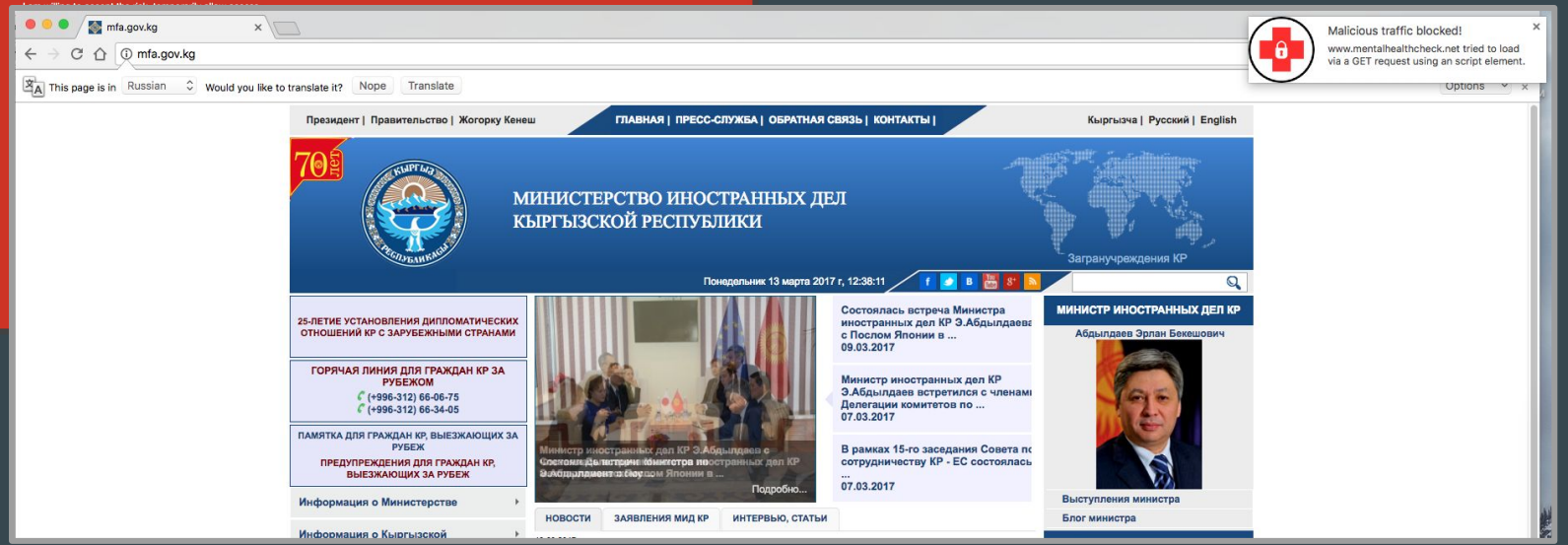


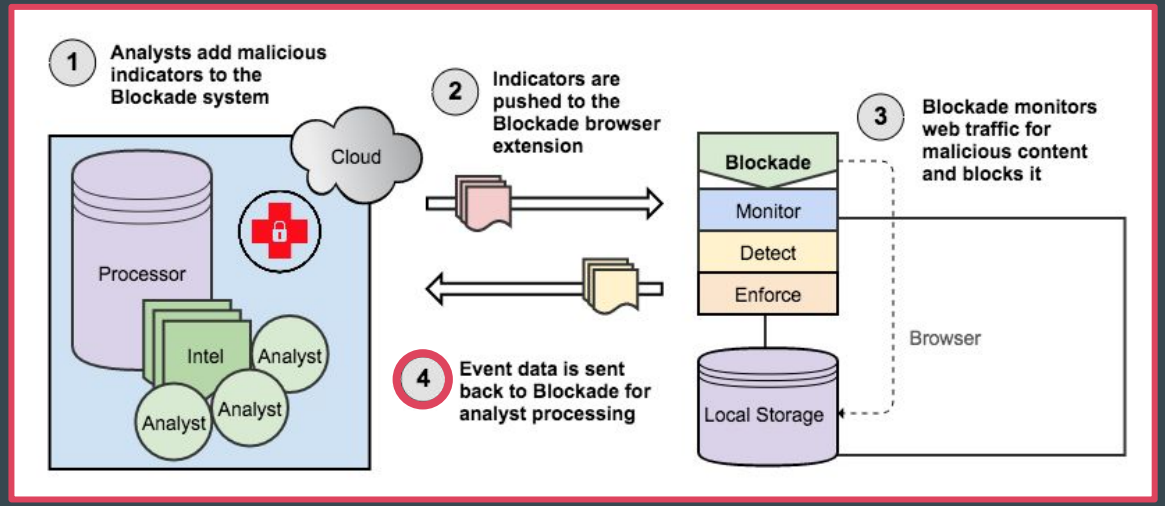
#3

- Extension leverages exposed browser APIs to monitor traffic
  - *webRequest.onBeforeRequest* is used to intercept all network requests **prior** any packet leaving the web browser (includes DNS prefetch and asynchronous requests)
- Request resources are parsed, hashed and checked against the local database
  - If there's a match, communications are redirected to local pages advising the user of the resource
  - In the event the request is part of a website, a pop-up will notify the user


Blockade Warning
Brandon
chrome-extension://fpafbnpdjmkjlebldajjjdefipfcmhod/resources/static/warning.html?redirect=https://phishing.evil.com/
Suspicious site reported!
Blockade has reported phishing.evil.com as suspicious. This website may try to trick you into doing something dangerous like installing software or revealing personal information (for example, passwords, phone numbers, or credit cards). View the raw details.
TAKE ME AWAY!


Malicious traffic blocked!
test.blockade.io tried to load via a GET request using an image element.


mfa.gov.kg
This page is in Russian
Would you like to translate it?
Nope
Translate
Malicious traffic blocked!
www.mentalhealthcheck.net tried to load via a GET request using an script element.
Президент | Правительство | Жогорку Кенеш
ГЛАВНАЯ | ПРЕСС-СЛУЖБА | ОБРАТНАЯ СВЯЗЬ | КОНТАКТЫ |
Кыргызча | Русский | English
70 лет
МИНИСТЕРСТВО ИНОСТРАННЫХ ДЕЛ КЫРГЫЗСКОЙ РЕСПУБЛИКИ
Загранучреждения КР
Понедельник 13 марта 2017 г, 12:38:11
25-ЛЕТИЕ УСТАНОВЛЕНИЯ ДИПЛОМАТИЧЕСКИХ ОТНОШЕНИЙ КР С ЗАРУБЕЖНЫМИ СТРАНАМИ
ГОРЯЧАЯ ЛИНИЯ ДЛЯ ГРАЖДАН КР ЗА РУБЕЖОМ
(+996-312) 66-06-75
(+996-312) 66-34-05
ПАМЯТКА ДЛЯ ГРАЖДАН КР, ВЫЕЗЖАЮЩИХ ЗА РУБЕЖ
ПРЕДУПРЕЖДЕНИЯ ДЛЯ ГРАЖДАН КР, ВЫЕЗЖАЮЩИХ ЗА РУБЕЖ
Информация о Министерстве
Информация о Кыргызской
Подробно...
Состоялась встреча Министра иностранных дел КР Э.Абдылдаева с Послом Японии в ...
09.03.2017
Министр иностранных дел КР Э.Абдылдаев встретился с членами Делегации комитетов по ...
07.03.2017
В рамках 15-го заседания Совета по сотрудничеству КР - ЕС состоялась ...
07.03.2017
НОВОСТИ
ЗАЯВЛЕНИЯ МИД КР
ИНТЕРВЬЮ, СТАТЬИ
МИНИСТР ИНОСТРАННЫХ ДЕЛ КР
Абдылдаев Эрлан Бекешович
Выступления министра
Блог министра

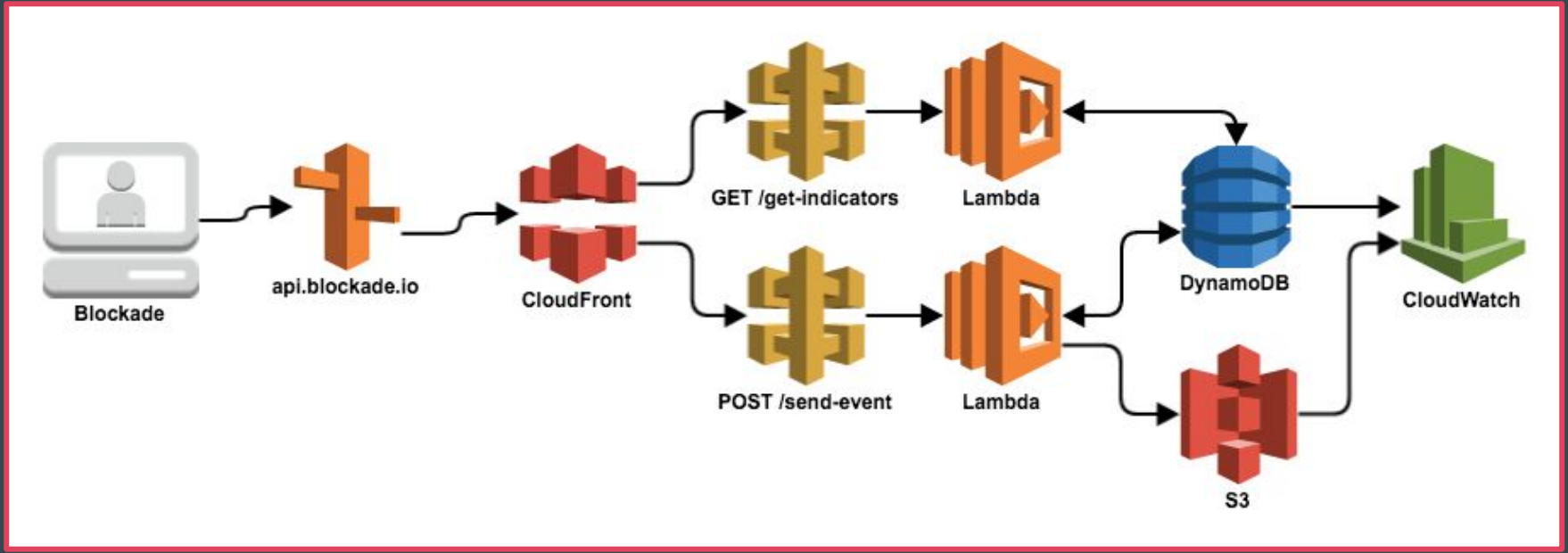


#4

- Details related to the blocking event are recorded and sent back to the cloud
  - Optional email address can be included in order to get in contact with the user
  - Allows analysts to investigate the threat further with context
- Built-in context menu that allows analysts to submit indicators while browsing
  - Data is sent directly to the selected cloud node, processed and push back down to the extension

Collection of data created by the extension and information collected from Chrome on the running environment. Note, the indicator is public in the payload since we obtained it via the network interception.

Alternative Deployment Strategy



Demo

Isn’t this just Google Safe Browsing (GSB)?

Yes, it’s similar, but with a few distinct benefits

- Blockade is open source and freely available to anyone
- Blockade is not backed by a product company
  - You control the indicators, users, management, etc.
- Blockade is targeted to only what’s in the database
- Blockade can feed data back to the operators
- Blockade requires nearly no change to user behavior to function

State of the Project

- Presently in a beta state and used by a few targeted groups
  - The Citizen Lab & Security Without Borders
- Looking for more analysts to contribute targeted indicators via API
  - Event data from browser hits will be shared and made available
- Looking for analysts or organizations to host their own cloud node
  - Potential alternative to deliver intelligence to users in near real-time
- Looking for activists, journalists, and other volunteers for testing
- Looking for developers to assist
  - Adding more capabilities for administrators and analysts
  - Porting the extension over to FireFox

Explore the Code: https://github.com/blockadeio/

Getting Access

- Chrome Extension - https://github.com/blockadeio/chrome_extension
- Website - https://github.com/blockadeio/website
- Analyst Toolbench - https://github.com/blockadeio/analyst_toolbench
- Cloud Node - https://github.com/blockadeio/cloud_node
- Firefox Extension - Coming soon

If you want to help, send mail to info@blockade.io or submit a pull request

Questions?