Brick

One small part of a layered, automation foundation

Why brick?

account abuse history

current app functionality

future app functionality

Resource Abuse

Examples

Ticket	Date	IP Addresses	User Agents
106387	2019-05	132	?
107413	2019-06	129	?
116454	2019-09	5	4,762
117007	2019-09	26	14
127868	2020-02	31	23,683

IP alerts: good

User Agent alerts: better

Current Splunk alerts/thresholds

- User Agents
  - 5 per 24 hours
  - 5 per 4 hours
  - 5 per hour
- IPs
  - 75 per 7 days
  - 15 per 7 days
- EZproxy status code 418
- EZproxy Admin User

Disabling user accounts: Manually

Technical

1. Notification
   - Splunk email alert
   - vendor email to Technical Services
2. Verify report
   - Splunk dashboard (often)
   - shell scripts (sometimes)
3. Update users.disabled.txt
4. Deploy users.disabled.txt
5. Terminate active user sessions (manually)

Procedural

1. Update tickets
2. Back & forth with Technical Services
3. Technical Services goes back & forth with the vendor
4. Access is restored

Purpose of this app

Past Experiences

- 6 pm on a Friday
- We're done for the day, logged out, "gone home"
- Uncapped abuse
- Angry vendor Monday

Purpose of this app

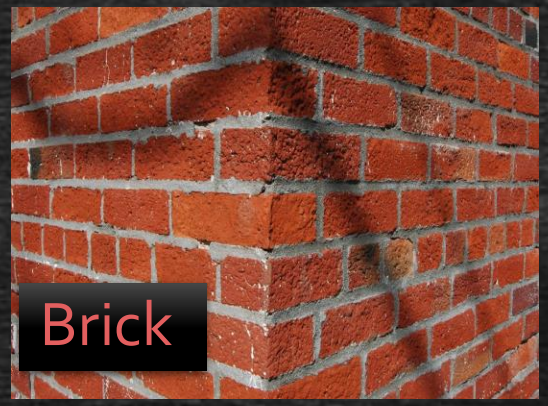
Future Experience

- *6 pm on a Friday*
- *We're done for the day, logged out, "gone home"*
- Abuse kicks up briefly
- Splunk sends alert
- This app* automatically disables the account, notifies us
- Abuse is greatly minimized

* plus supporting tooling

brick Workflow

splunk>



FAIL2BAN

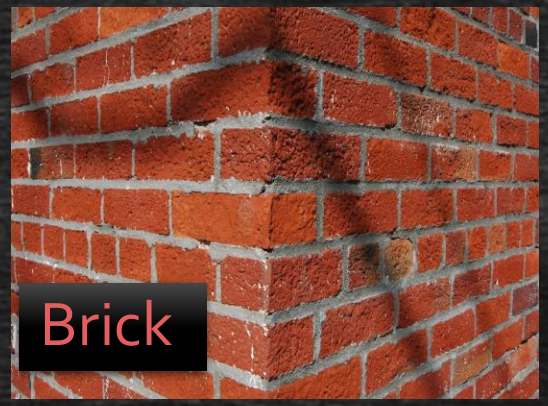
Abusive activity

EZproxy®

Microsoft Teams

brick Workflow

splunk>



FAIL2BAN

Traffic logs
(always flowing)

Abusive activity

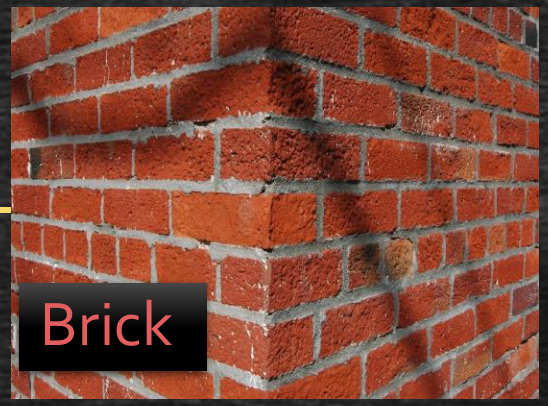
EZproxy®

Microsoft Teams

brick Workflow

splunk>

Splunk alert



FAIL2BAN

Traffic logs
(always flowing)

Abusive activity

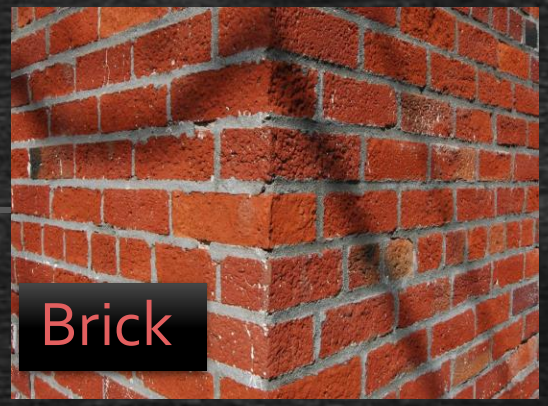
EZproxy®

Microsoft Teams

brick Workflow

splunk>

Splunk alert



Process alert

Traffic logs
(always flowing)

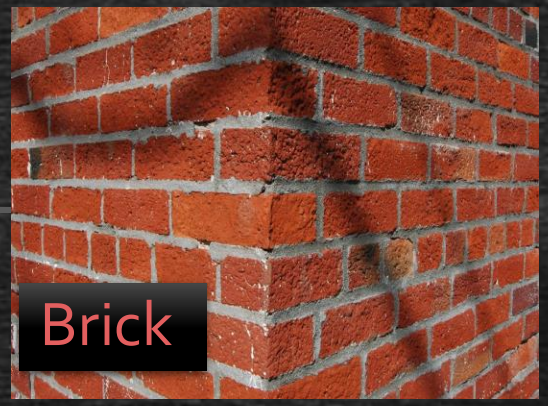
Abusive activity

EZproxy®

FAIL2BAN

Microsoft Teams

brick Workflow



Log report received

splunk>

Splunk alert

Process alert

Send receipt notifications

X

Traffic logs (always flowing)

Abusive activity

EZproxy

Microsoft Teams

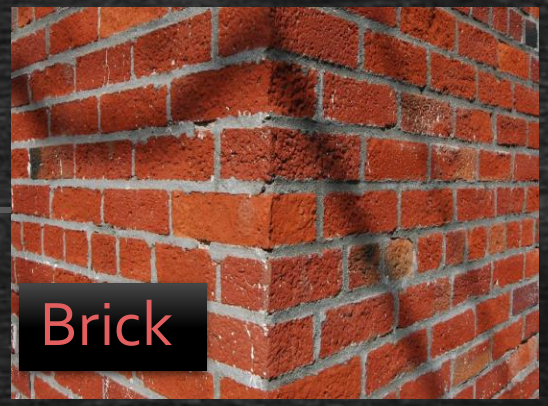
FAIL2BAN

brick Workflow

splunk>

Splunk alert

Traffic logs
(always flowing)



Log report received

Log disable action

*Log ignore action**

Process alert

Send receipt notifications

Disable User

FAIL2BAN

Microsoft Teams

EZproxy®

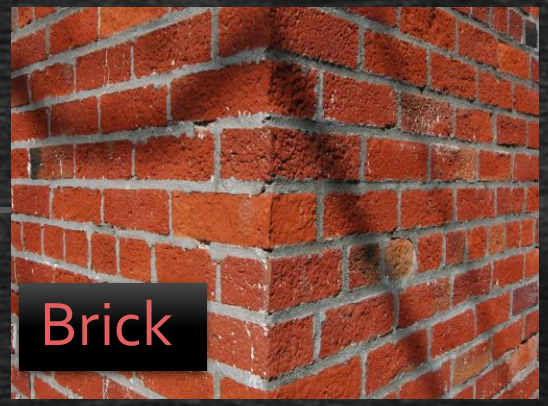
Abusive activity

**brick can be configured to ignore specific user accounts or IP Addresses.*

brick Workflow

splunk>

Splunk alert



Log report received

Log disable action

*Log ignore action**

Send disable notifications

Process alert

Send receipt notifications

Disable User

Traffic logs (always flowing)

FAIL2BAN

Microsoft Teams

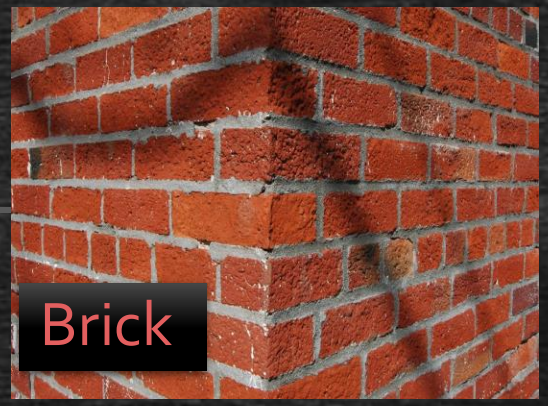
EZproxy®

Abusive activity

brick Workflow

splunk>

Splunk alert



Log report received

Log disable action

*Log ignore action**

Send disable notifications

FAIL2BAN

Temp IP ban (in order to force session timeout)

Process alert

Send receipt notifications

Disable User

Traffic logs (always flowing)

X

Microsoft Teams

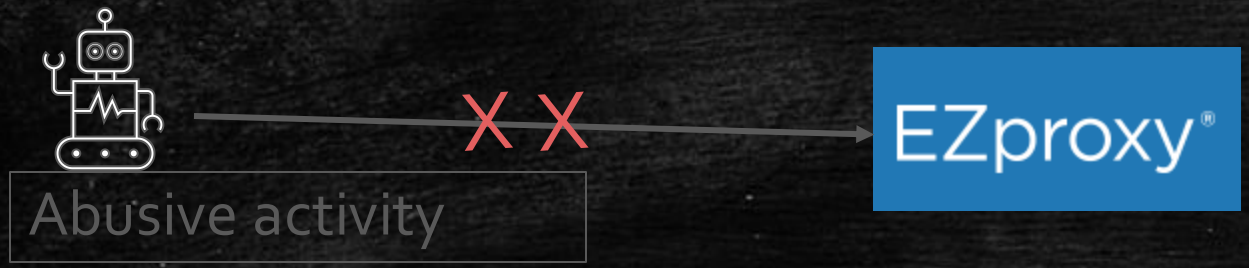
EZproxy®

X X

Abusive activity

What next?

- User login session times out, terminating account access.
- Disabled account entry "sticks" until manually removed.



Demonstration time!

- First payload with as-is demo settings
- Duplicate or repeat Splunk alert
- Enable Teams Notifications
- Same test username, different IP Address
- Ignored username, different IP Address
- Ignored IP Address, different username

Improvements

Planned

- Email notifications directly from brick
  - Analogue to Teams notifications
- Additional endpoints (e.g., list disabled users)

Potential

- LDAP - add disabled user accounts to AD group
- Warning-only behavior for low-confidence alerts
- Refactor to send/receive payloads to and from other services such as Service Now (e.g., update availability), Redmine (e.g., create tickets)

What Now?

1. Deploy to EZproxy test server and enable live payloads from Splunk
2. Start the conversation regarding reducing the MaxLifetime EZproxy setting (controls session inactivity timer)
3. Additional demos of this application to other groups (e.g., Technical Services, Reference, Leadership?)
4. Start planning production deployment

Credit, References, Sources, ...

- "Brick" image
  - https://www.flickr.com/photos/sfantti/239849911/
- Splunk
  - https://www.splunk.com/
- EZproxy
  - https://www.oclc.org/en/ezproxy.html
- Fail2ban
  - https://www.fail2ban.org/
- Brick
  - https://github.com/atcooo5/brick