29th ANNUAL FIRST CONFERENCE

SAN JUAN
PUERTO RICO
JUNE 11-16, 2017

FIGHTING PIRATES AND PRIVATEERS

WWW.FIRST.ORG

You’re Leaking: Incident Response in the World of DevOps

Jerry Dixon & Levi Gundert

29th ANNUAL FIRST CONFERENCE
SAN JUAN PUERTO RICO

JERRY DIXON

@jwdixonjr

- **CROWDSTRIKE**
  Chief Information Security Officer
- **AMERICAN EXPRESS**
  Vice President, Cyber Threat Intelligence & Incident Response
- **CISCO SYSTEMS**
  Director, Incident Response
- **US DEPARTMENT OF HOMELAND SECURITY**
  Director: National Cyber Security Division

29th ANNUAL FIRST CONFERENCE
SAN JUAN PUERTO RICO

LEVI GUNDERT

@levigundert

- **RECORDED FUTURE**
  Vice President, Threat Intelligence & Strategy
- **FIDELITY INVESTMENTS**
  Vice President, Cyber Threat Intelligence
- **CISCO SYSTEMS**
  Technical Leader, Talos
- **U.S. SECRET SERVICE – LOS ANGELES ECTF**
  Special Agent

Incident Response Ops

- Monitoring your security infrastructure
  - Billion plus events a month!
  - Triage
  - Monitoring for Data ExFil
  - Insider Threat (UBA)
  - Operationalizing Threat Intelligence
- Managing the incident queues
  - Email
  - Incident Hotline
  - Ticketing system
  - Triage
- <u>What's Missing?</u>

DevOps Defined

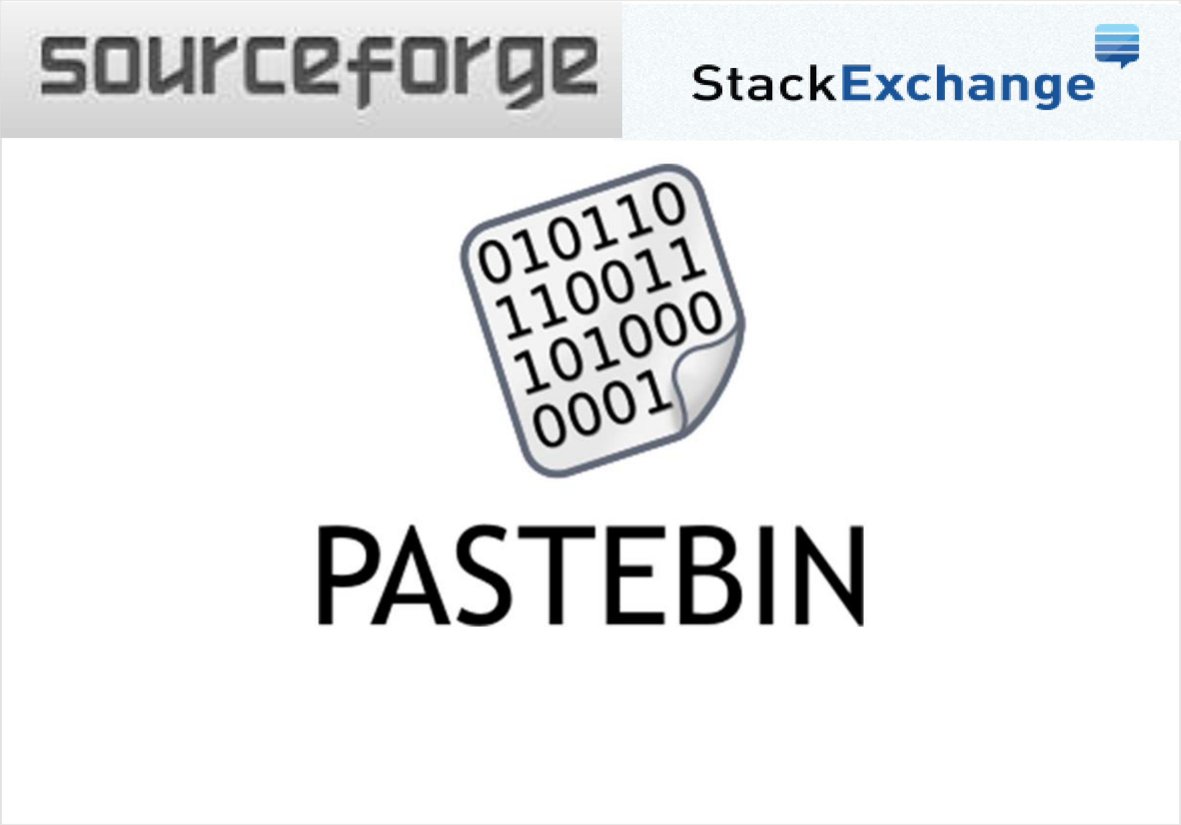
- Blending of Development efforts and IT operations to support rapid development plus faster delivery of products or services.
- Many organizations have moved to this model in the financial sector, corporate world, and pioneered in high tech firms
- Foster greater collaboration
- Lots of risk to consider and approach to protecting your organization!

DevOps Gone Bad

- Developers demanding broad access & administrative rights
- “Silly IT or InfoSec team, we want unfettered access to the Internet”
  - “Trust Us!”
  - “We shouldn’t be bogged down with the same restrictions as everyone else”
  - “I don’t want to fill out an exception request.” “So what if we’re regulated or a public company. I’m special!”
- I own the code!

You’re Leaking!

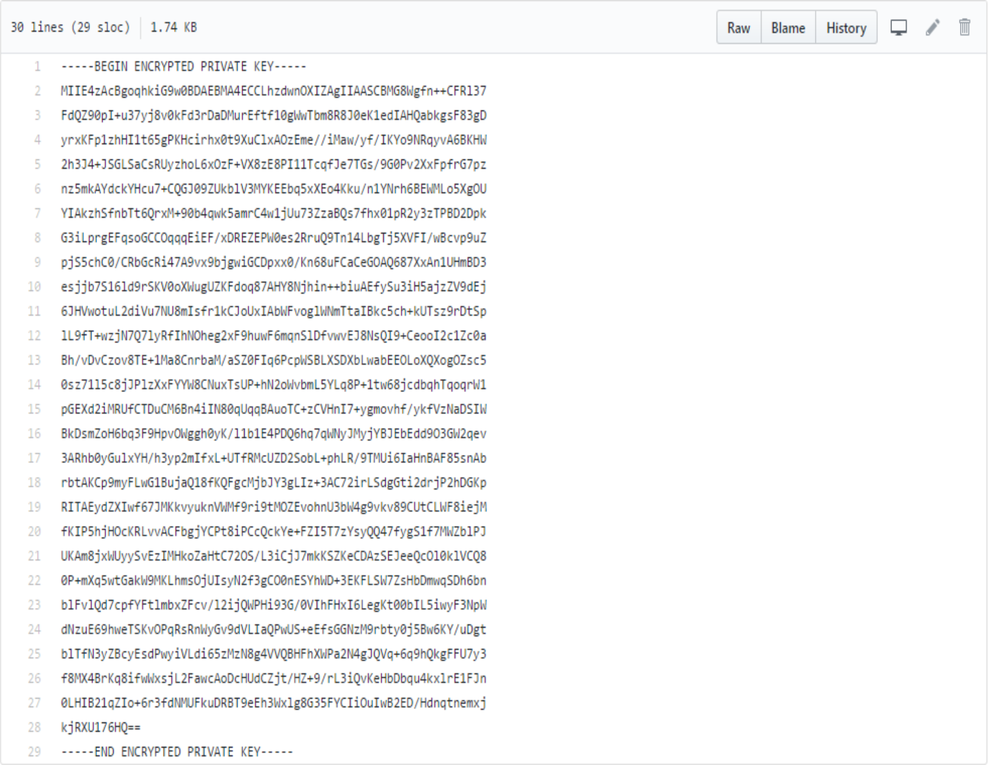
- SSH-Keys
- API-Keys
- Digital Certificates
- Authorization Keys
- PGP Private Keys
- Sensitive architecture diagrams
- Sensitive names of critical applications or systems



GITHUB

Let’s go Hunting!
Why bother, our developers can be trusted!
Or can they?

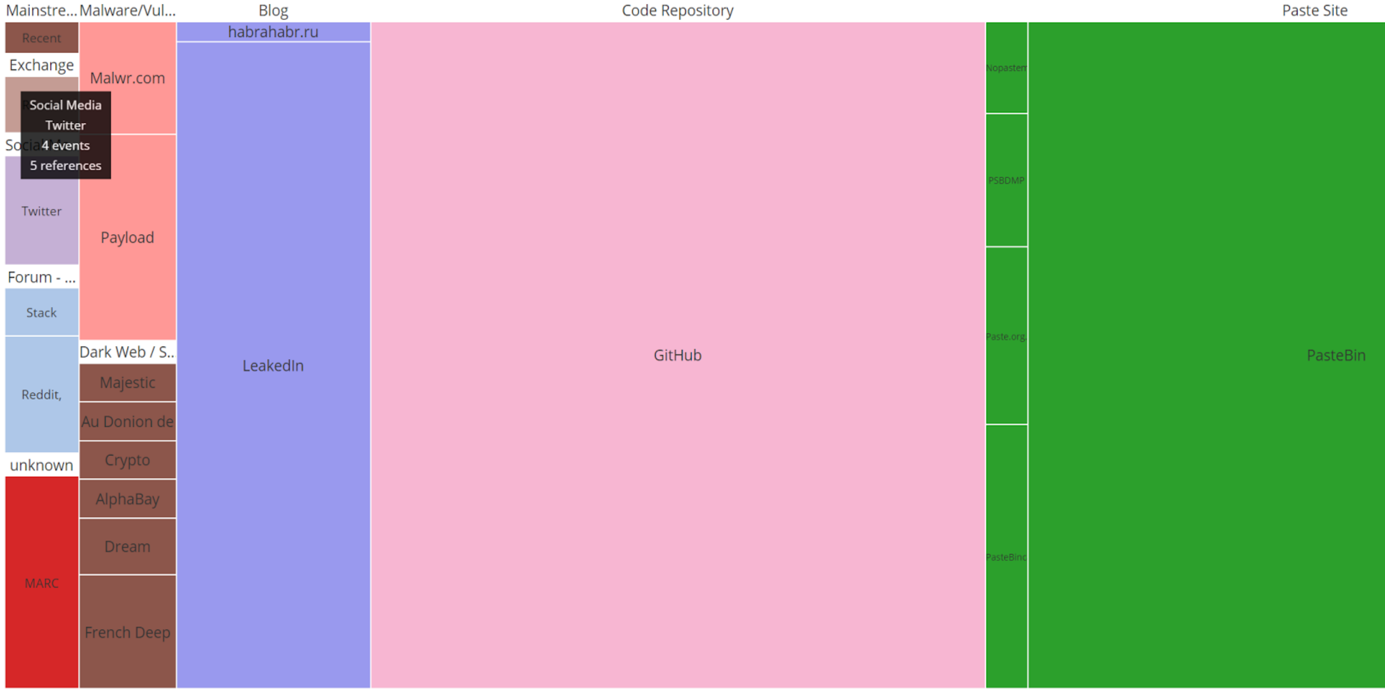
Repo Gold Nuggets: Help your Adversary!



30 lines (29 sloc) | 1.74 KB

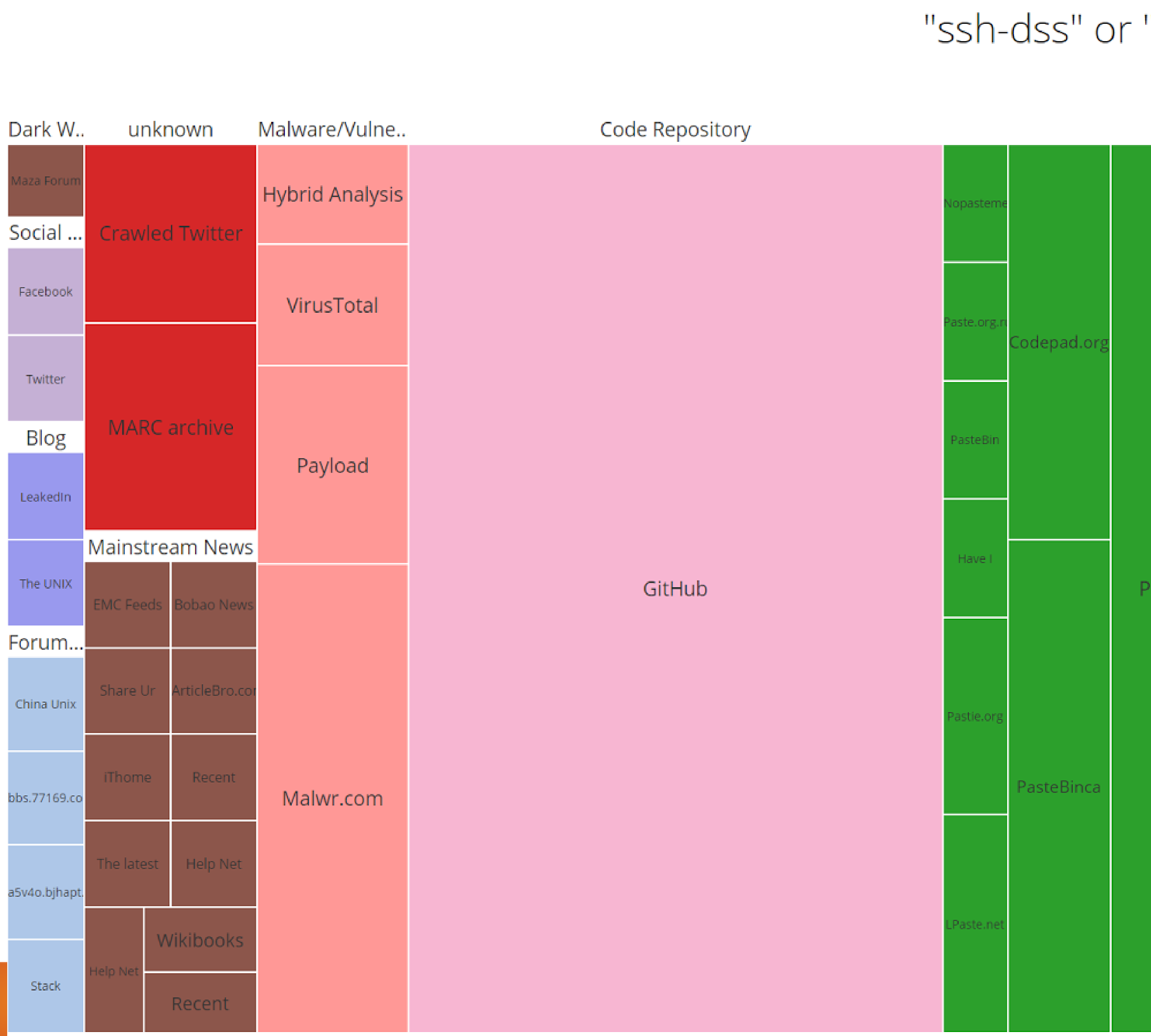
```
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIE4zAcBgoqhkiG9w0BDAEBMA4ECCLhzdwnOXIZAgIIAASCBMG8Wgfn++CFR137
FdQZ90pI+u37yj8v0kFd3rDaDMurEftf10gWwTbm8R8J0eK1edIAHQabkgsF83gD
yrxKFp1zhHI1t65gPKHcirhx0t9XuClxAOzEme//iMaw/yf/IKYo9NRqyvA6BKHW
2h3J4+JSGLSaCsRUyzhoL6xOzF+VX8zE8PI11TcqfJe7TGs/9G0Pv2XxFpfrG7pz
nz5mkAYdckYHcu7+CQGJ09ZUkblV3MYKEEbq5xXEo4Kku/n1YNrh6BEWMLo5XgOU
YIAkzhSfnbTt6QrxM+90b4qwk5amrC4w1jUu73ZzaBQs7fhx01pR2y3zTPBD2Dpk
G3iLprgEFqsoGCCOqqqEiEF/xDREZEPW0es2RruQ9Tn14LbgTj5XVFI/wBcvp9uZ
pjS5chC0/CRbGcRi47A9vx9bjgwiGCDpxx0/Kn68uFCaCeGOAQ687XxAn1UHmBD3
esjjb7S161d9rSKV0oXWugUZKFdoq87AHY8Njhin++biuAEfySu3iH5ajzZV9dEj
6JHVwotuL2diVu7NU8mIsfr1kCJoUxIAbWFvoglWNmTtaIBkc5ch+kUTsz9rDtSp
1L9fT+wzjN7Q71yRfIhNOheg2xF9huwF6mqnSlDfvwvEJ8NsQI9+CeooI2c1Zc0a
Bh/vDvCzov8TE+1Ma8CnrbaM/aSZ0FIq6PcpWSBLXSDXbLwabEEOLoXQXogOZsc5
0sz7115c8jJPlzXxFYYW8CNuxTsUP+hN2oWvbmL5YLq8P+1tw68jcdbqhTqoqrW1
pGEXd2iMRUfCTDuCM6Bn4iIN80qUqqBAuoTC+zCVHnI7+ygmovhf/ykfVzNaDSIW
BkDsmZoH6bq3F9HpvOWggh0yK/11b1E4PDQ6hq7qWNyJMyjYBJEbEdd9O3GW2qev
3ARhb0yGulxYH/h3yp2mIfxL+UTfRMcUZD2SobL+phLR/9TMUi6IaHnBAF85snAb
rbtAKCp9myFLwG1BujaQ18fKQFgcMjbJY3gLIz+3AC72irLSdgGti2drjP2hDGKp
RITAEydZXIwf67JMKkvyuknVWMf9ri9tMOZEvohnU3bW4g9vkv89CUtCLWF8iejM
fKIP5hjHOcKRLvvACFbgjYCPt8iPCcQckYe+FZI5T7zYsyQQ47fygS1f7MWZb1PJ
UKAm8jxWUyySvEzIMHkoZaHtC72OS/L3iCjJ7mkKSZKeCDAzSEJeeQcO10k1VCQ8
0P+mXq5wtGakW9MKLhmsOjUIsyN2f3gCO0nESYhWD+3EKFLSW7ZsHbDmwqSDh6bn
blFvlQd7cpfYFtlmbxZFcv/12ijQWPHi93G/0VIhFHxI6LegKt00bIL5iwyF3NpW
dNzuE69hweTSKvOPqRsRnWyGv9dVLIaQPwUS+eEfsGGNzM9rbty0j5Bw6KY/uDgt
blTfN3yZBcyEsdPwyiVLdi65zMzN8g4VVQBHFhXWPa2N4gJQVq+6q9hQkgFFU7y3
f8MX4BrKq8ifwWxsjL2FawcAoDcHUdCZjt/HZ+9/rL3iQvKeHbDbqu4kxlrE1FJn
0LHIB21qZIo+6r3fdNMUFkuDRBT9eEh3Wxlg8G35FYCIiOuIwB2ED/Hdnqtnemxj
kjRXU176HQ==
-----END ENCRYPTED PRIVATE KEY-----
```

"BEGIN PGP PRIVATE KEY BLOCK"

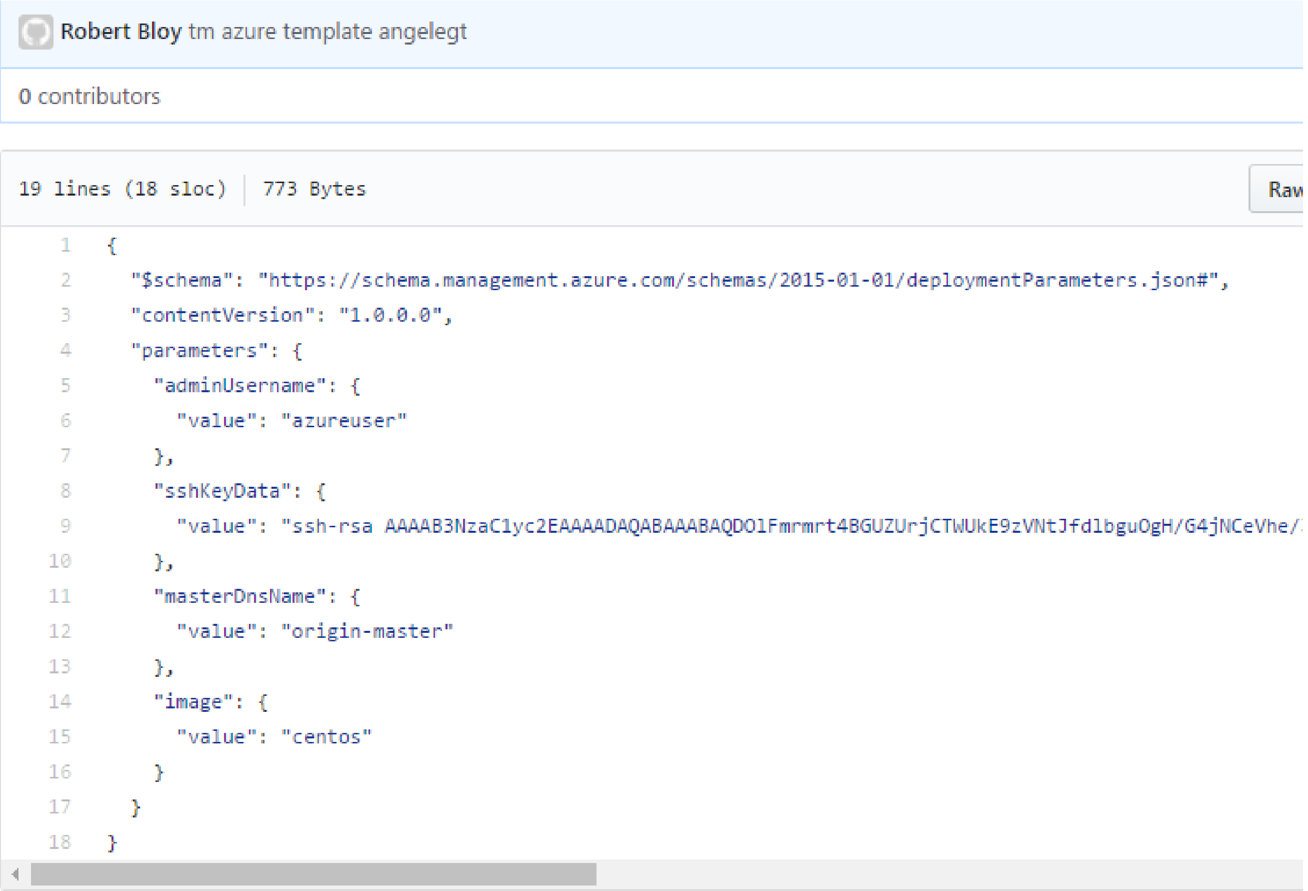


Repo Gold Nuggets: Help your Adversary!

- 5809 references for “auth token”
- 36,582 references for certificates using “begin certificate” and 425 references for “Begin encrypted private key”



Deployment Templates are common



Robert Bloy tm azure template angelegt

0 contributors

19 lines (18 sloc) | 773 Bytes

```
{
  "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentParameters.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "adminUsername": {
      "value": "azureuser"
    },
    "sshKeyData": {
      "value": "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDO1Fmrmrt4BGUZUrjCTWUkE9zVNtJfdlbguOgH/G4jNCeVhe/
    },
    "masterDnsName": {
      "value": "origin-master"
    },
    "image": {
      "value": "centos"
    }
  }
}
```

- You’ll find SSH-Keys
- API Keys
- Auth CERTS
- IP addresses – with or without FQDN (great for recon)
- Vendor executables tailored to customers
- Service Accounts (my favorite)
- VPN or AD Credentials

What are the drivers?

- Culture & age
  - Information should be free & always available
  - Crowdsourcing development
  - It’s my computer!
  - It’s my code!
  - I should be able to take my code with me wherever I go. Besides, I wrote it!
  - Privacy means different things to different folks

Incident Response & Detection in DevOps

- If you’re not hunting public code repositories for sensitive information on a daily basis you’re making it easier for your adversaries
- It’s easy to get lost in monitoring your perimeter and internal infrastructure but we have to remember developers love to use public code repositories, not just for code, but architecture diagrams, and often as a backup drive to their computer (Lots of stories here)
- If you work in a locked-down environment developers will sometimes upload sensitive IP/code to Github & then download at home to work on it versus lugging their work laptop around then download again at the office. Often “Too Cheap” to purchase a private account!

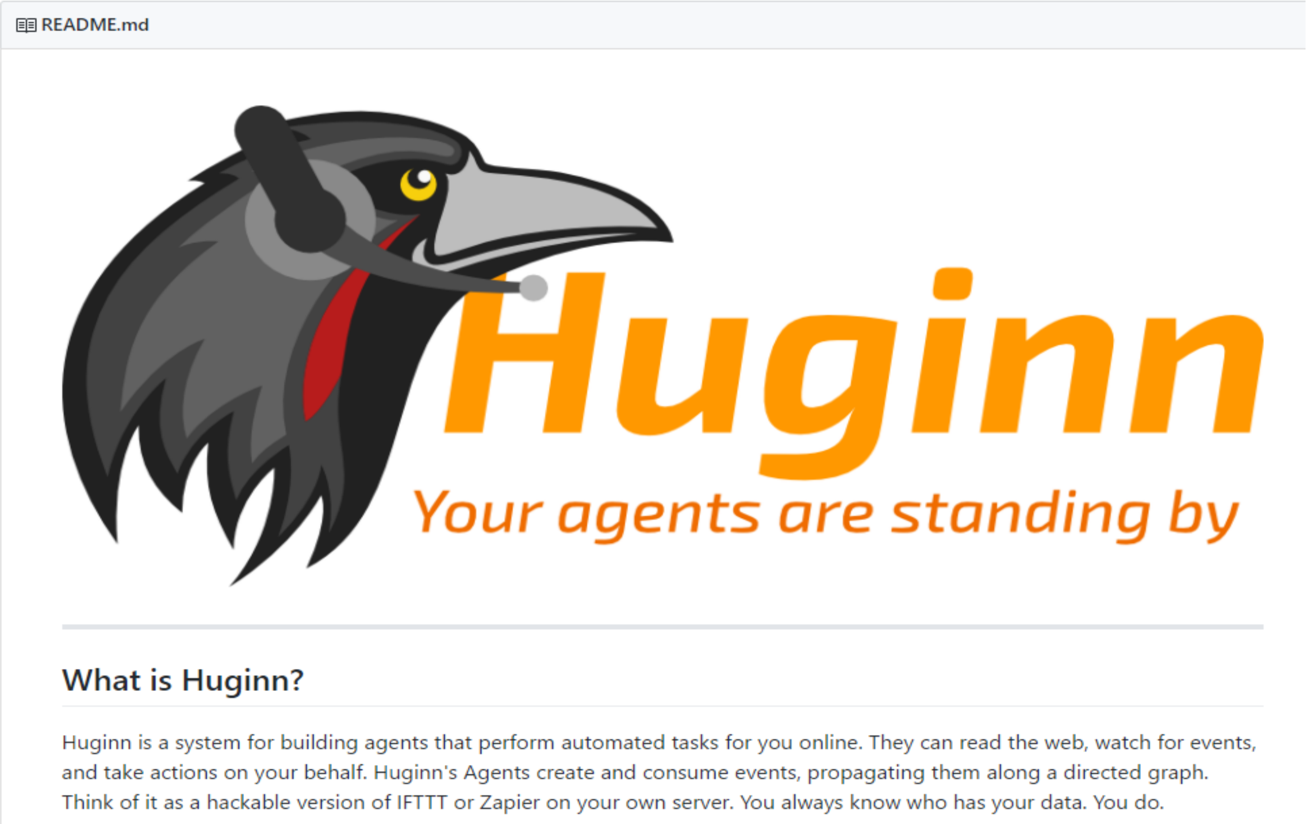
Let’s talk tools

- GITHUB Dorks - is quite powerful and useful feature and can be used to search sensitive data on the repositories. Collection of github dorks that can reveal sensitive personal and/or organizational information such as private keys, credentials, authentication tokens, etc. This list is supposed to be useful for assessing security and performing pen-testing of systems.
- Source: https://github.com/techgaun/github-dorks

Another tool

- GITROB - a command line tool which can help organizations and security professionals find sensitive information lingering in publicly available files on GitHub. The tool will iterate over all public organization and member repositories and match filenames against a range of patterns for files that typically contain sensitive or dangerous information.
- Source: https://github.com/michenriksen/gitrob/blob/master/README.md
- Helps with Org monitoring

Another Open Source Option



README.md

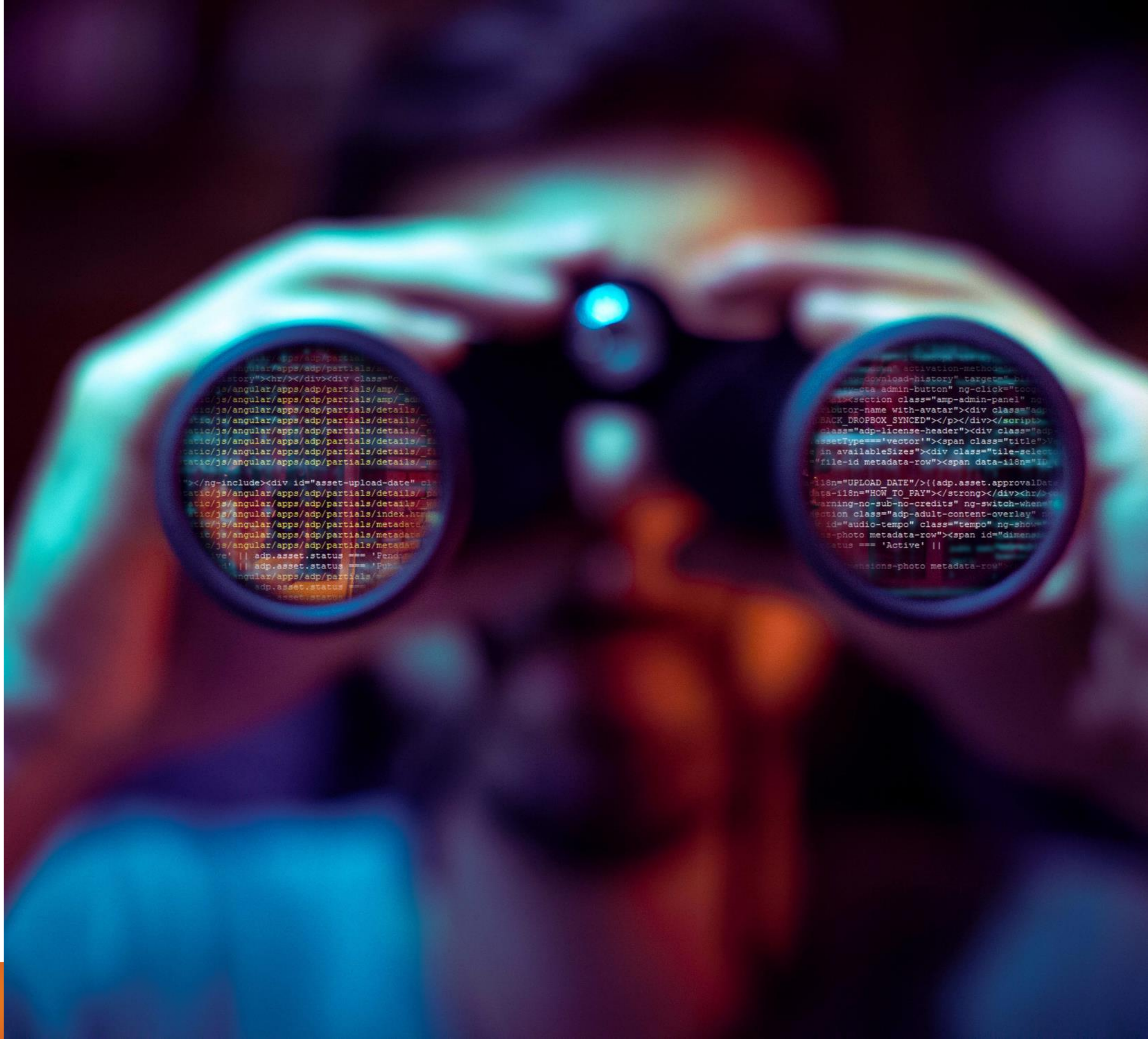
What is Huginn?

Huginn is a system for building agents that perform automated tasks for you online. They can read the web, watch for events, and take actions on your behalf. Huginn's Agents create and consume events, propagating them along a directed graph. Think of it as a hackable version of IFTTT or Zapier on your own server. You always know who has your data. You do.

- Huginn is a system for building agents that perform automated tasks for you online. They can read the web, watch for events, and take actions on your behalf. Huginn's Agents create and consume events, propagating them along a directed graph. Think of it as a hackable version of IFTTT or Zapier on your own server.
- Source: https://github.com/huginn/huginn

So now we’ve talked tools, Now What?

- Build an IR Playbook
- Ensure your monitoring / detection is working
- Automate your hunting to drive operational efficiency
- Track metrics & incident stats to show “adult supervision” is still needed. But incorporate the DevOps team in building the guardrails



Data Leak Playbook for Public Repo’s

- Identify the developer quickly. Have them take the information down if they’re still with the organization.
- Monitor internal systems talking to repo’s.
- Have the security team for the Repo on “speed dial” to help with take-down
- Did I mention there is a researcher in Brazil that mirrors a certain public repo. By the way, he won’t take down the info.

Data Leak Playbook for Public Repo's

- Have a plan to quickly change api-keys, ssh-keys, rotate certificates, or change passwords. Exercise it in a table-top to ensure all folks are prepared.
    - Did you think about your cloud environment?
    - Your internal infrastructure?
    - Application owners / Devs
- Have a containment plan ready to go.
- Leverage your security tools to see who is doing sync's to repos or manually going there.

Crisis Response

- Have that escalation plan ready to go if you have a data leak. Especially if you can’t get the data down.
- By the way, did I mention you should also be monitoring social media? You need to quickly determine if there is chatter about your exposure of sensitive information.
- Have a communications plan in place for inside the organization, media, regulators, or your customers depending on the situation.
- Stand up that War Room and ensure your crisis response team is engaged (corp comms, legal, IT, Privacy, Global Security, etc)

Questions?