netskope
THREAT LABS

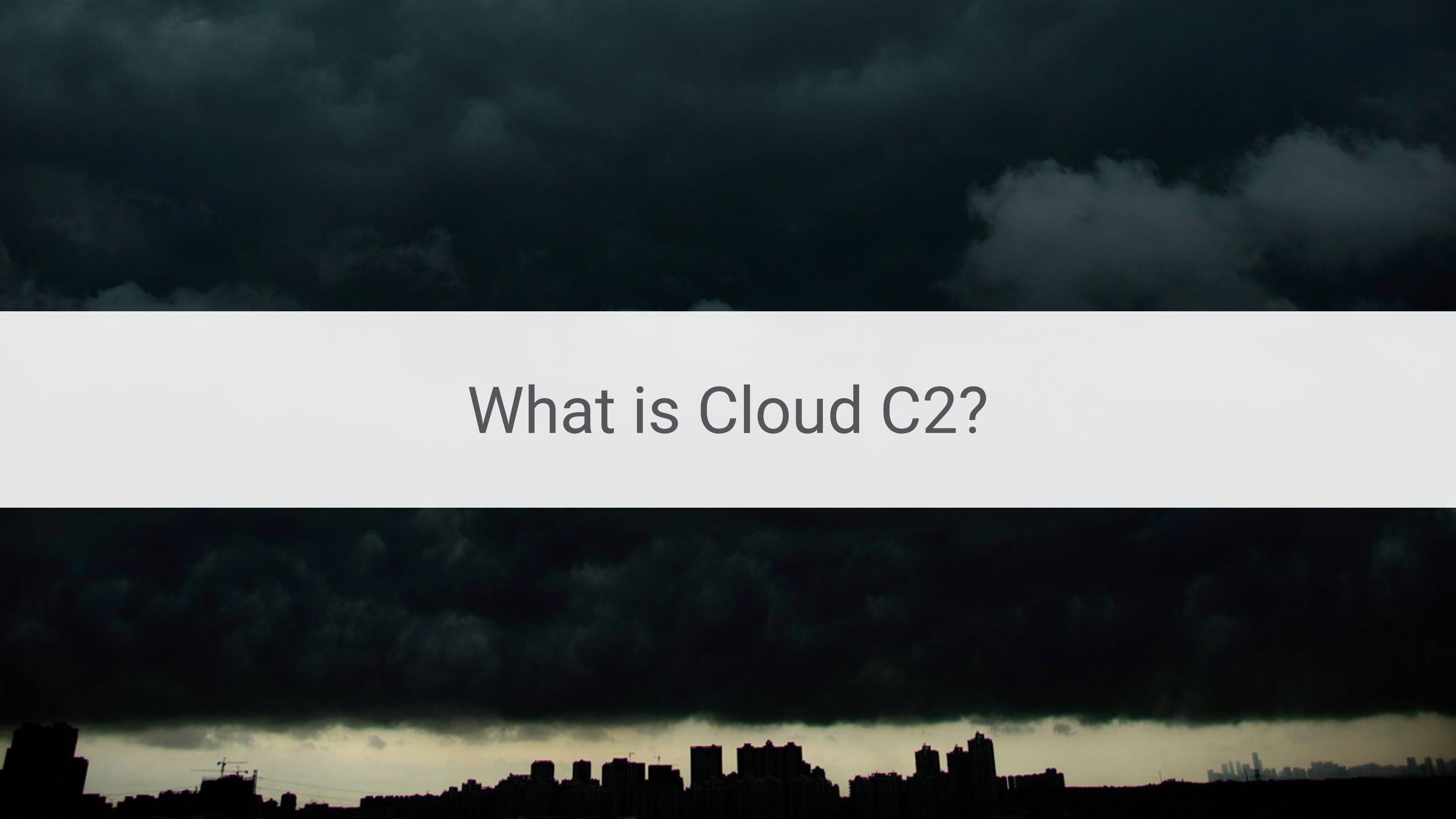
Detecting cloud command and control

Dagmawi Mulugeta
Threat Researcher @ Netskope Threat Labs

October 25th 2022
Swiss Cyber Storm

Outline

- What is Cloud C2?
- Why is Cloud C2 hard to detect?
- Lab environment
- Detection approach
- Demonstration



What is Cloud C2?

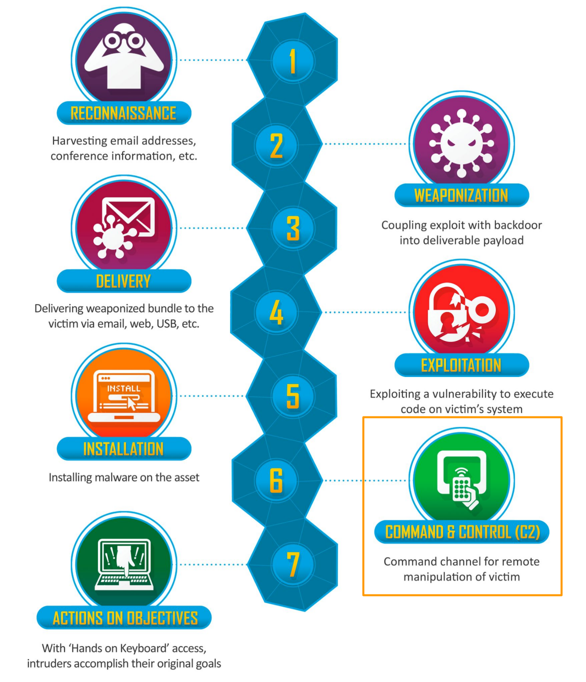
Command and Control

- Stage in the Cyber Kill Chain

- Traditionally, involves a compromised device polling a server for commands

- Via mediums like HTTPs and DNS directly to an attacker controlled server

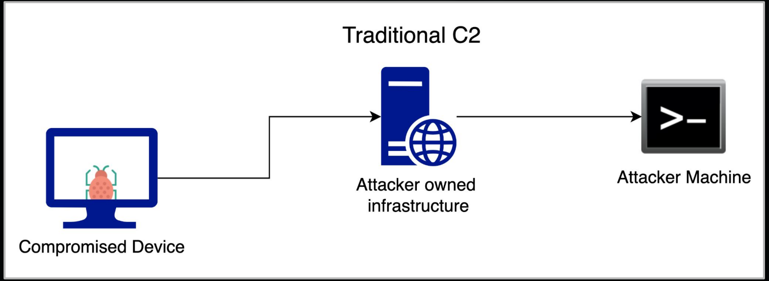
- Example frameworks include Cobalt Strike and PowerShell Empire


1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

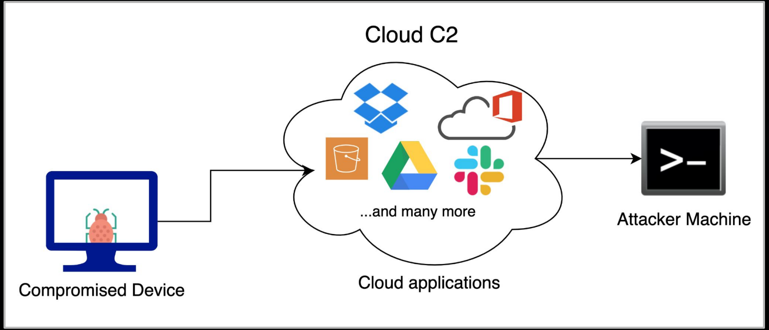
Source: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Cloud Command and Control (Cloud C2)

- **Traditional C2**
  - Attackers setting up their own servers, domains, etc.
  - Tough to detect, but can be identified via IP / domain blocklists



- **Cloud C2**
  - (ab)Use a cloud applications as a command and control channel
  - Very minimal setup
  - Even tougher to detect since traffic blends in with normal app usage

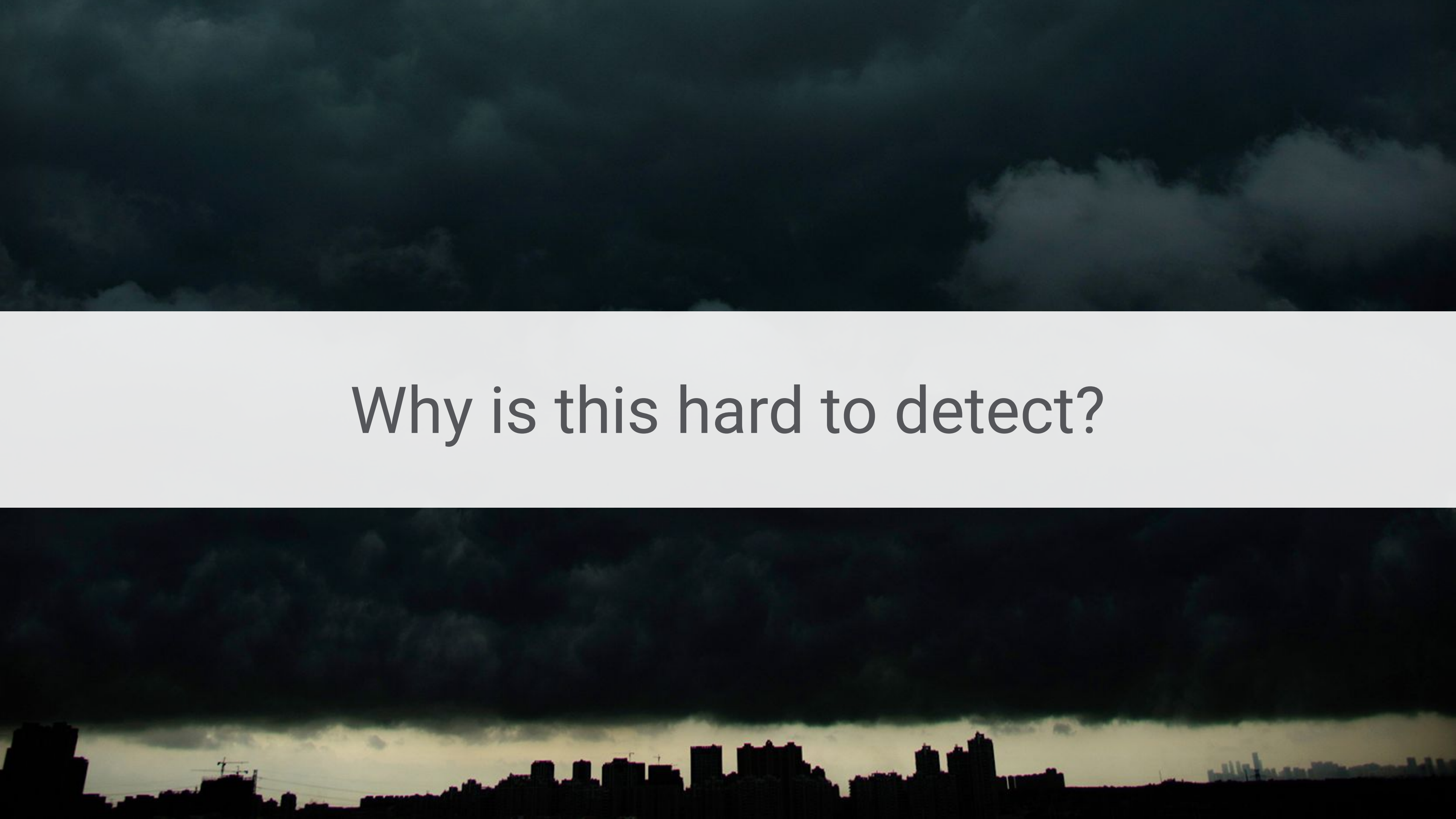


Real world examples

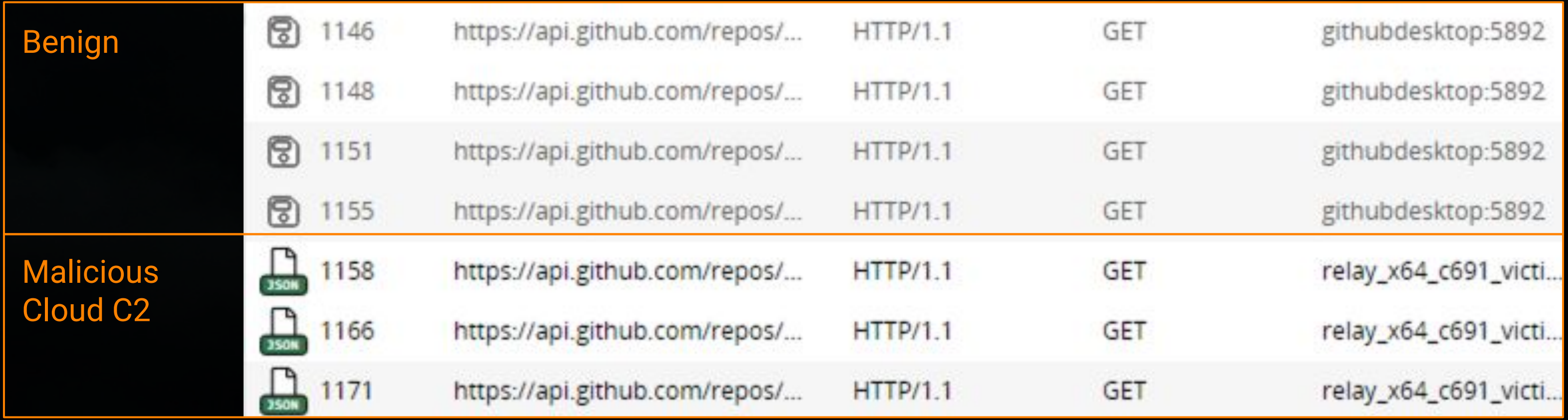
- Some examples of malware and cloud apps they abuse:
    - BoxCaon, Nimble Mamba and Crutch have used ***DropBox*** for C2 communications
    - Graphite and BLUELIGHT abuse ***OneDrive*** for C2
    - Aclip abused messenger application ***Slack's*** API for C2
    - BLACKCOFFEE and Lazarus abused ***Github*** to obfuscate its C2 traffic
    - Pawn Storm abuses ***Google Drive*** via a RAT
    - CozyCar and ROKRAT abuse ***Twitter*** as a main and backup C2 channel
    - Comnie uses ***Tumblr*** and ***BlogSpot*** to mask C2 traffic
    - FIN7 used services like ***Google Docs***, ***Google Scripts***, and ***Pastebin*** for C2
    - MuddyWater abused ***OneHub*** to distribute remote access tools
    - Sandworm abused the ***Telegram Bot API*** to send and receive commands
    - GIFShell is abusing ***Microsoft Teams*** for C2

- A more detailed list can be found on MITRE's page

Why is this hard to detect?

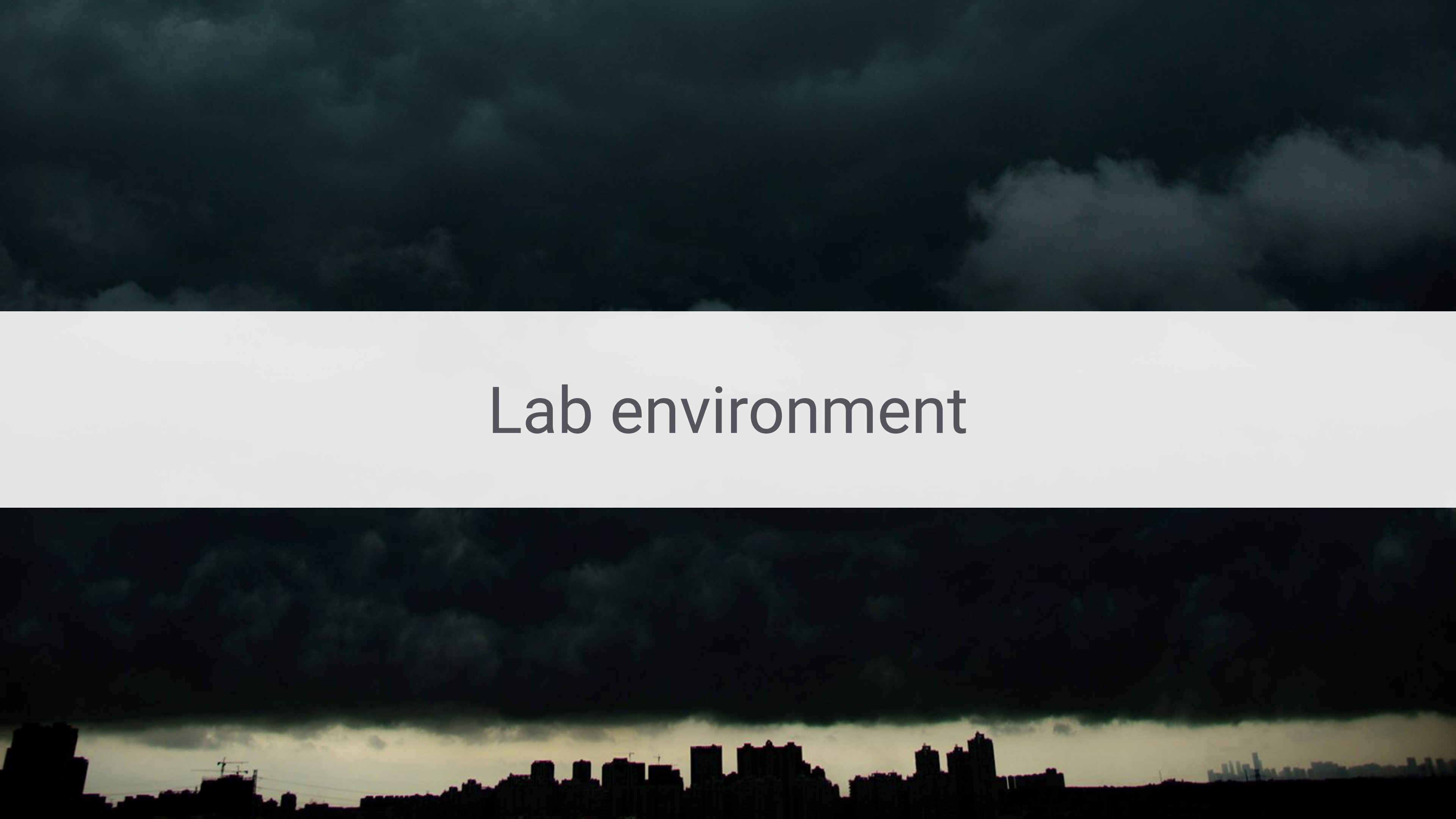


Why is this hard to detect?



Benign		1146	https://api.github.com/repos/...	HTTP/1.1	GET	githubdesktop:5892
		1148	https://api.github.com/repos/...	HTTP/1.1	GET	githubdesktop:5892
		1151	https://api.github.com/repos/...	HTTP/1.1	GET	githubdesktop:5892
		1155	https://api.github.com/repos/...	HTTP/1.1	GET	githubdesktop:5892
Malicious Cloud C2	JSON	1158	https://api.github.com/repos/...	HTTP/1.1	GET	relay_x64_c691_victi...
	JSON	1166	https://api.github.com/repos/...	HTTP/1.1	GET	relay_x64_c691_victi...
	JSON	1171	https://api.github.com/repos/...	HTTP/1.1	GET	relay_x64_c691_victi...

- Both malicious and benign traffic is going to the same domain
- The domain is a valid cloud provider domain
- The traffic to the domain is encrypted using the cloud provider’s certificate



Lab environment

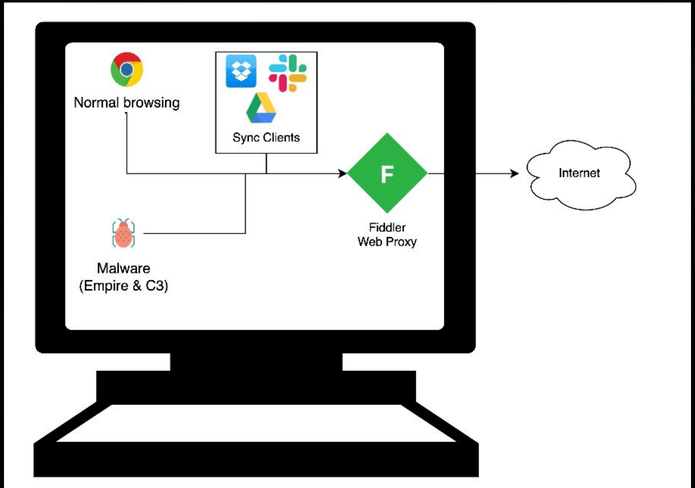
Tools

Empire: Empire is a PowerShell and Python 3 post-exploitation framework (https://github.com/BC-SECURITY/Empire)

Custom Command and Control (C3): Framework for rapid prototyping of custom C2 channels and providing integration to offensive toolkits like Cobalt Strike and Covenant (https://github.com/FSecureLABS/C3)

Fiddler: A web debugging proxy tool that gives insight into the HTTPs traffic from a machine by decrypting the communication between the client and server. (https://www.telerik.com/fiddler)

Setup

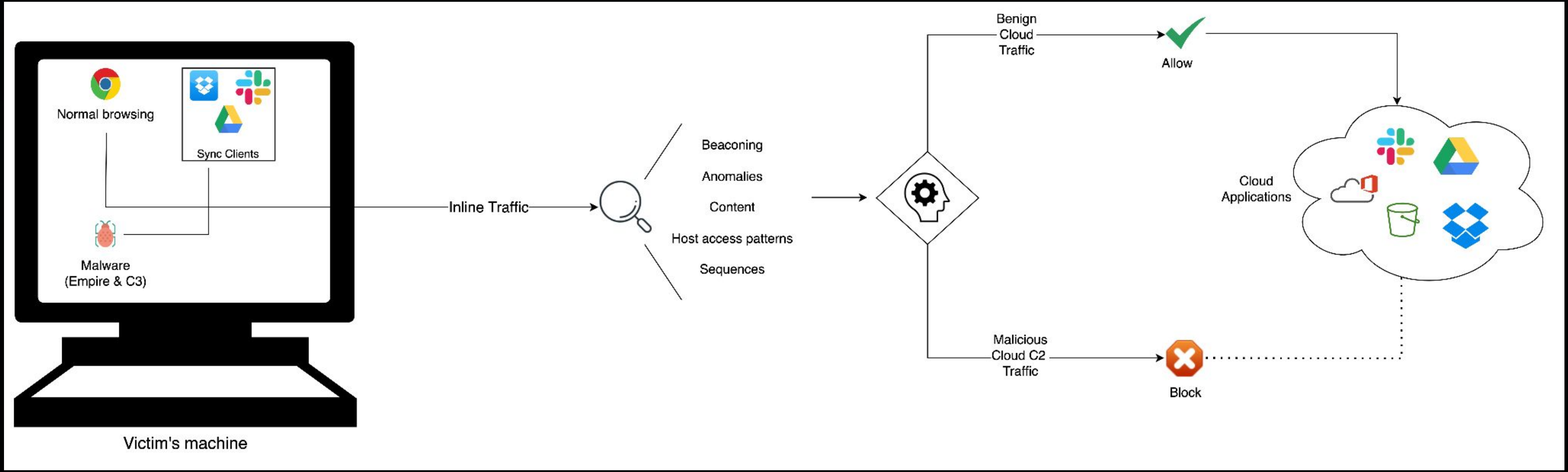


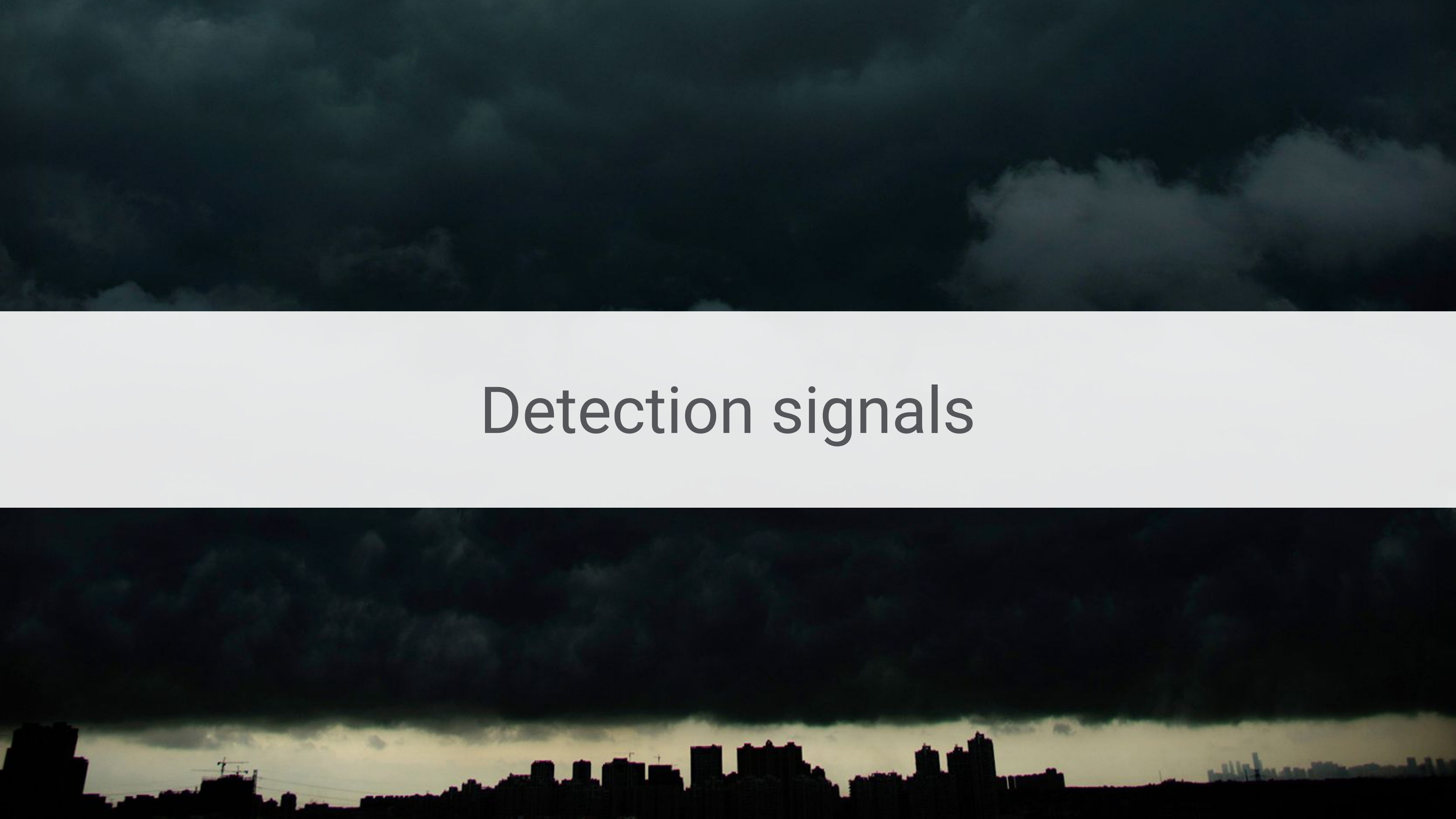
- Benign processes running: Browsers and native apps (sync clients) were connected to various cloud applications

- Malicious processes running: Used C3 and Empire to generate the “malicious” cloud C2 traffic

- Fiddler was running to capture these web requests and data was exported as a .saz file for analysis

Overview


Normal browsing
Sync Clients
Malware
(Empire & C3)
Victim's machine
Inline Traffic
Beaconing
Anomalies
Content
Host access patterns
Sequences
Benign
Cloud
Traffic
Allow
Malicious
Cloud C2
Traffic
Block
Cloud
Applications

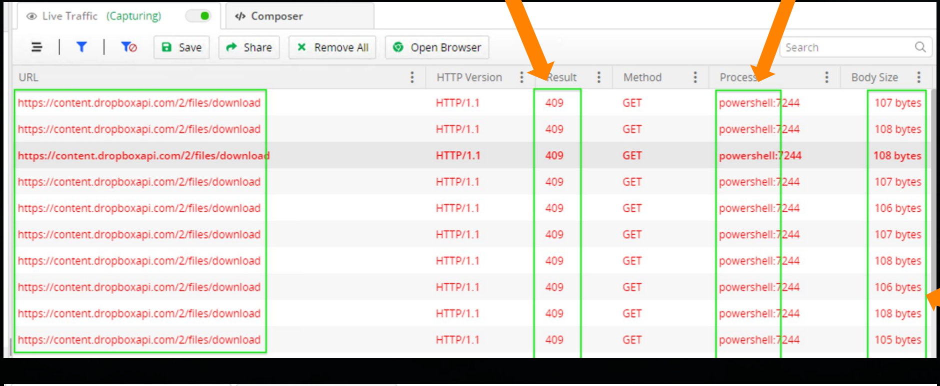


Detection signals

Beaconing

Repeated requests and responses

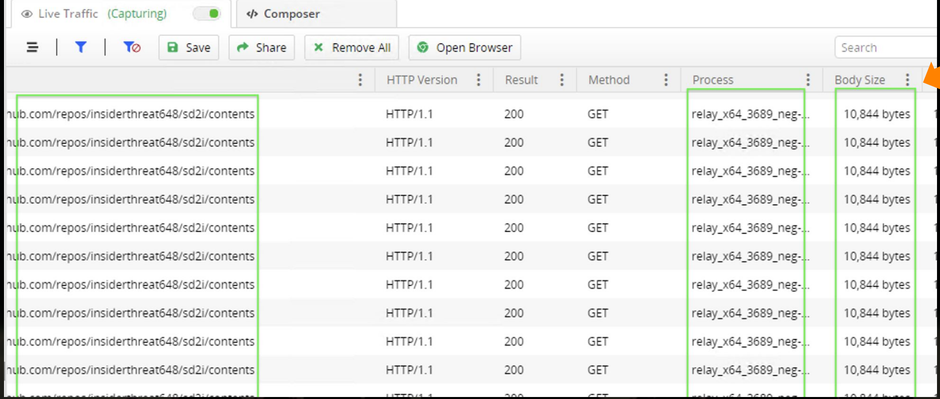
Unusual process making request



URL	HTTP Version	Result	Method	Process	Body Size
https://content.dropboxapi.com/2/files/download	HTTP/1.1	409	GET	powershell:7244	107 bytes
https://content.dropboxapi.com/2/files/download	HTTP/1.1	409	GET	powershell:7244	108 bytes
https://content.dropboxapi.com/2/files/download	HTTP/1.1	409	GET	powershell:7244	108 bytes
https://content.dropboxapi.com/2/files/download	HTTP/1.1	409	GET	powershell:7244	107 bytes
https://content.dropboxapi.com/2/files/download	HTTP/1.1	409	GET	powershell:7244	106 bytes
https://content.dropboxapi.com/2/files/download	HTTP/1.1	409	GET	powershell:7244	107 bytes
https://content.dropboxapi.com/2/files/download	HTTP/1.1	409	GET	powershell:7244	108 bytes
https://content.dropboxapi.com/2/files/download	HTTP/1.1	409	GET	powershell:7244	106 bytes
https://content.dropboxapi.com/2/files/download	HTTP/1.1	409	GET	powershell:7244	108 bytes
https://content.dropboxapi.com/2/files/download	HTTP/1.1	409	GET	powershell:7244	105 bytes

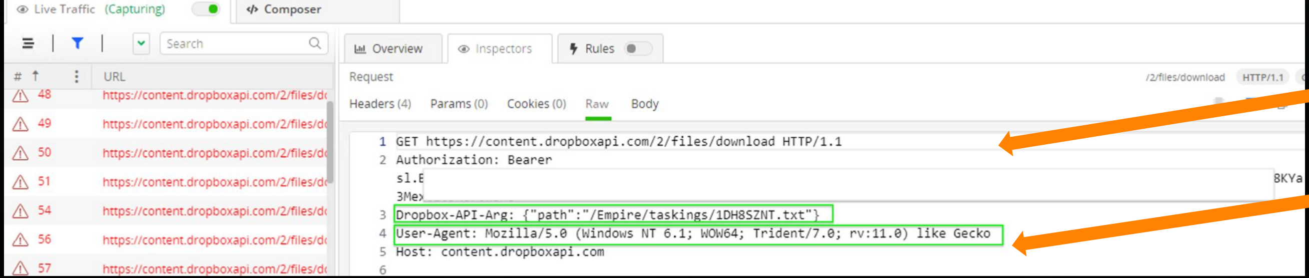
Frequent checks to same URL

Not much deviation in data size



	HTTP Version	Result	Method	Process	Body Size
hub.com/repos/insiderthreat648/sd2i/contents	HTTP/1.1	200	GET	relay_x64_3689_neg-...	10,844 bytes
hub.com/repos/insiderthreat648/sd2i/contents	HTTP/1.1	200	GET	relay_x64_3689_neg-...	10,844 bytes
hub.com/repos/insiderthreat648/sd2i/contents	HTTP/1.1	200	GET	relay_x64_3689_neg-...	10,844 bytes
hub.com/repos/insiderthreat648/sd2i/contents	HTTP/1.1	200	GET	relay_x64_3689_neg-...	10,844 bytes
hub.com/repos/insiderthreat648/sd2i/contents	HTTP/1.1	200	GET	relay_x64_3689_neg-...	10,844 bytes
hub.com/repos/insiderthreat648/sd2i/contents	HTTP/1.1	200	GET	relay_x64_3689_neg-...	10,844 bytes
hub.com/repos/insiderthreat648/sd2i/contents	HTTP/1.1	200	GET	relay_x64_3689_neg-...	10,844 bytes
hub.com/repos/insiderthreat648/sd2i/contents	HTTP/1.1	200	GET	relay_x64_3689_neg-...	10,844 bytes
hub.com/repos/insiderthreat648/sd2i/contents	HTTP/1.1	200	GET	relay_x64_3689_neg-...	10,844 bytes
hub.com/repos/insiderthreat648/sd2i/contents	HTTP/1.1	200	GET	relay_x64_3689_neg-...	10,844 bytes

Anomalies

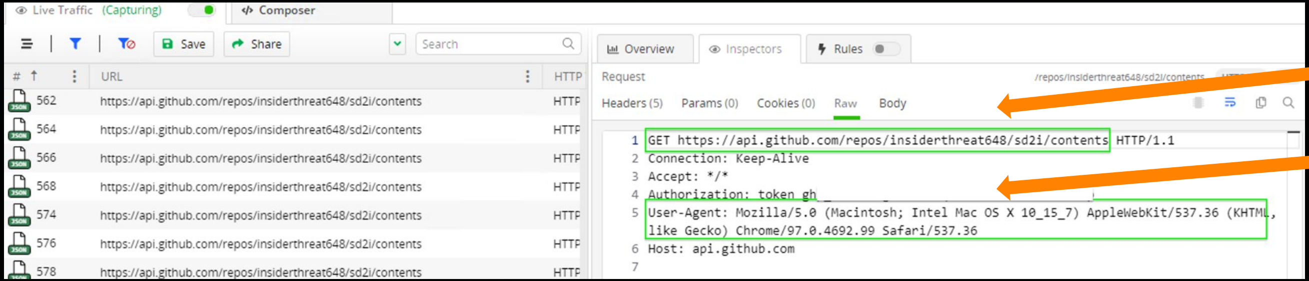


#	URL
48	https://content.dropboxapi.com/2/files/dc
49	https://content.dropboxapi.com/2/files/dc
50	https://content.dropboxapi.com/2/files/dc
51	https://content.dropboxapi.com/2/files/dc
54	https://content.dropboxapi.com/2/files/dc
56	https://content.dropboxapi.com/2/files/dc
57	https://content.dropboxapi.com/2/files/dc

```
GET https://content.dropboxapi.com/2/files/download HTTP/1.1
Authorization: Bearer
sl.E[redacted]8KYa
3Mex
Dropbox-API-Arg: {"path":"/Empire/taskings/1DH8SZNT.txt"}
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: content.dropboxapi.com
```

Unusual entities (i.e., slack channels, github repos, dropbox folders)

Unusual user agent for the user's machine (or associated with known malware)



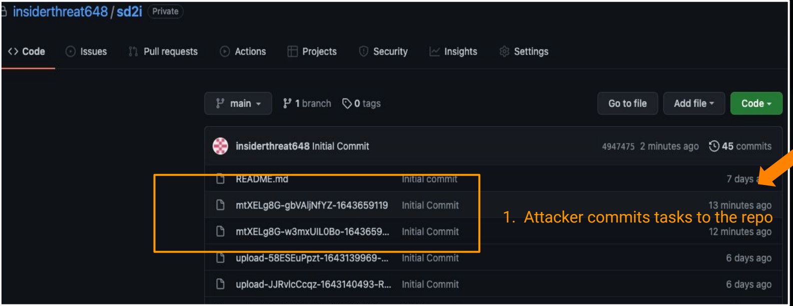
#	URL	HTTP
562	https://api.github.com/repos/insiderthreat648/sd2i/contents	HTTP
564	https://api.github.com/repos/insiderthreat648/sd2i/contents	HTTP
566	https://api.github.com/repos/insiderthreat648/sd2i/contents	HTTP
568	https://api.github.com/repos/insiderthreat648/sd2i/contents	HTTP
574	https://api.github.com/repos/insiderthreat648/sd2i/contents	HTTP
576	https://api.github.com/repos/insiderthreat648/sd2i/contents	HTTP
578	https://api.github.com/repos/insiderthreat648/sd2i/contents	HTTP

```
GET https://api.github.com/repos/insiderthreat648/sd2i/contents HTTP/1.1
Connection: Keep-Alive
Accept: */*
Authorization: token gh[redacted]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/97.0.4692.99 Safari/537.36
Host: api.github.com
```

Unusual username used to login to the app

Unusual authentication method (E.g., Org uses SSO for GitHub, but this auth was with token)

Content

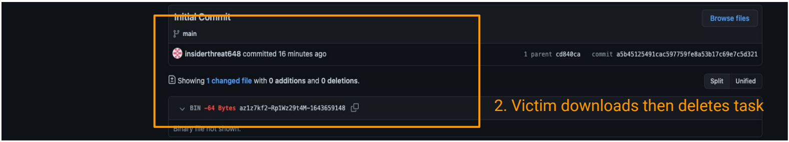


insiderthreat648 / sd2i Private

insiderthreat648 Initial Commit 4947475 2 minutes ago 45 commits

README.md	Initial commit	7 days a
mtXELg8G-gbVAljNfYZ-1643659119	Initial Commit	13 minutes ago
mtXELg8G-w3mxUIL0Bo-1643659...	Initial Commit	12 minutes ago
upload-58ESEuPpzt-1643139969-...	Initial Commit	6 days ago
upload-JJRvlcCcqz-1643140493-R...	Initial Commit	6 days ago

1. Attacker commits tasks to the repo



Initial Commit

main

insiderthreat648 committed 16 minutes ago

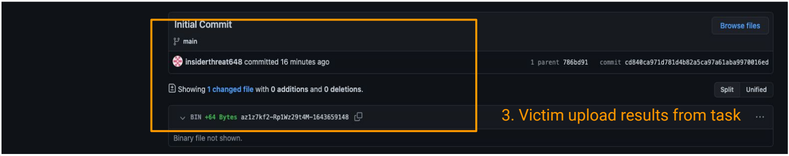
1 parent cd840ca commit a5b45125491cac597759fe8a53b17c69e7c5d321

Showing 1 changed file with 0 additions and 0 deletions.

```
BIN -64 Bytes az1z7kf2-Rp1Wz29t4M-1643659148
```

Binary file not shown.

2. Victim downloads then deletes task



Initial Commit

main

insiderthreat648 committed 16 minutes ago

1 parent 786bd91 commit cd840ca971d781d4b82a5ca97a61aba9970016ed

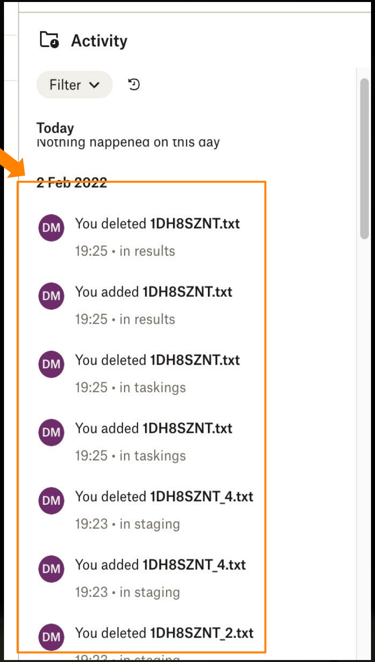
Showing 1 changed file with 0 additions and 0 deletions.

```
BIN +64 Bytes az1z7kf2-Rp1Wz29t4M-1643659148
```

Binary file not shown.

3. Victim upload results from task

Encrypted / encoded files being repeatedly uploaded and downloaded



Activity

Today
Nothing happened on this day

2 Feb 2022

DM You deleted 1DH8SZNT.txt
19:25 • in results

DM You added 1DH8SZNT.txt
19:25 • in results

DM You deleted 1DH8SZNT.txt
19:25 • in taskings

DM You added 1DH8SZNT.txt
19:25 • in taskings

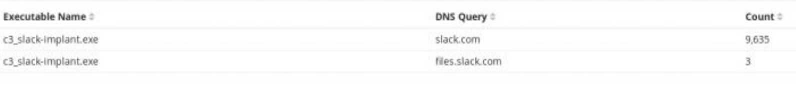
DM You deleted 1DH8SZNT_4.txt
19:23 • in staging

DM You added 1DH8SZNT_4.txt
19:23 • in staging

DM You deleted 1DH8SZNT_2.txt
19:23 • in staging

Host access patterns

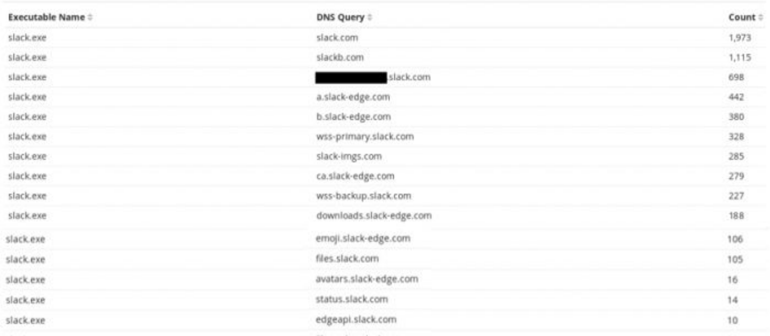
Unusual host (no one in the company uses slack, but seeing slack.com) with lack of referrers



Executable Name	DNS Query	Count
c3_slack-implant.exe	slack.com	9,635
c3_slack-implant.exe	files.slack.com	3

Malware

Volume in host lookups (the real slack.exe has more variation in domain names)



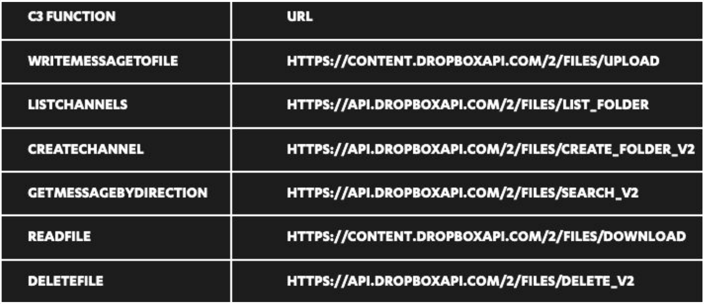
Executable Name	DNS Query	Count
slack.exe	slack.com	1,973
slack.exe	slackb.com	1,115
slack.exe	[redacted].slack.com	698
slack.exe	a.slack-edge.com	442
slack.exe	b.slack-edge.com	380
slack.exe	wss-primary.slack.com	328
slack.exe	slack-imgs.com	285
slack.exe	ca.slack-edge.com	279
slack.exe	wss-backup.slack.com	227
slack.exe	downloads.slack-edge.com	188
slack.exe	emoji.slack-edge.com	106
slack.exe	files.slack.com	105
slack.exe	avatars.slack-edge.com	16
slack.exe	status.slack.com	14
slack.exe	edgeapi.slack.com	10

Actual Slack

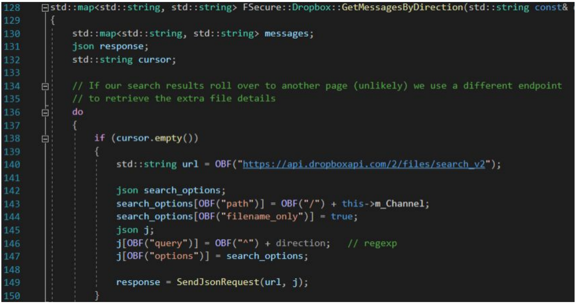
Source: https://labs.withsecure.com/blog/hunting-for-c3/

Sequences

Flag known hard coded endpoints



C3 FUNCTION	URL
WRITEMESSAGETOFILE	HTTPS://CONTENT.DROPBOXAPI.COM/2/FILES/UPLOAD
LISTCHANNELS	HTTPS://API.DROPBOXAPI.COM/2/FILES/LIST_FOLDER
CREATECHANNEL	HTTPS://API.DROPBOXAPI.COM/2/FILES/CREATE_FOLDER_V2
GETMESSAGEBYDIRECTION	HTTPS://API.DROPBOXAPI.COM/2/FILES/SEARCH_V2
READFILE	HTTPS://CONTENT.DROPBOXAPI.COM/2/FILES/DOWNLOAD
DELETEFILE	HTTPS://API.DROPBOXAPI.COM/2/FILES/DELETE_V2



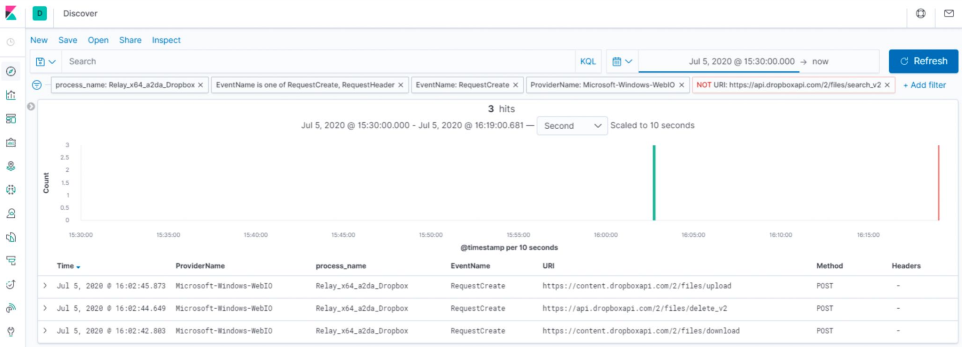
```
std::map<std::string, std::string> FSecure::Dropbox::GetMessagesByDirection(std::string const&
{
    std::map<std::string, std::string> messages;
    json response;
    std::string cursor;

    // If our search results roll over to another page (unlikely) we use a different endpoint
    // to retrieve the extra file details
    do
    {
        if (cursor.empty())
        {
            std::string url = OBF("https://api.dropboxapi.com/2/files/search_v2");

            json search_options;
            search_options[OBF("path")] = OBF("/") + this->m_Channel;
            search_options[OBF("filename_only")] = true;
            json j;
            j[OBF("query")] = OBF("^") + direction;   // regexp
            j[OBF("options")] = search_options;

            response = SendJsonRequest(url, j);
        }
```

Identify known sequences
(i.e., Download → Delete → Upload)



Jul 5, 2020 @ 15:30:00.000 → now

process_name: Relay_x64_a2da_Dropbox × EventName is one of RequestCreate, RequestHeader × EventName: RequestCreate × ProviderName: Microsoft-Windows-WebIO × NOT URI: https://api.dropboxapi.com/2/files/search_v2 ×

3 hits

Jul 5, 2020 @ 15:30:00.000 - Jul 5, 2020 @ 16:19:00.681 — Second Scaled to 10 seconds

Time	ProviderName	process_name	EventName	URI	Method	Headers
Jul 5, 2020 @ 16:02:45.873	Microsoft-Windows-WebIO	Relay_x64_a2da_Dropbox	RequestCreate	https://content.dropboxapi.com/2/files/upload	POST	-
Jul 5, 2020 @ 16:02:44.649	Microsoft-Windows-WebIO	Relay_x64_a2da_Dropbox	RequestCreate	https://api.dropboxapi.com/2/files/delete_v2	POST	-
Jul 5, 2020 @ 16:02:42.803	Microsoft-Windows-WebIO	Relay_x64_a2da_Dropbox	RequestCreate	https://content.dropboxapi.com/2/files/download	POST	-

Source: https://labs.f-secure.com/blog/attack-detection-fundamentals-c2-and-exfiltration-lab-3

List of signals used (select)

Low number of domains contacted

Low number of referred traffic

Known Cloud C2 domains contacted

Encrypted & encoded content

Lack of deviation between requests

Unusual authentication method

Unusual user agent

Unusual repos

Unusual usernames

Unusual slack channels, bots, and apps

Threshold based detector

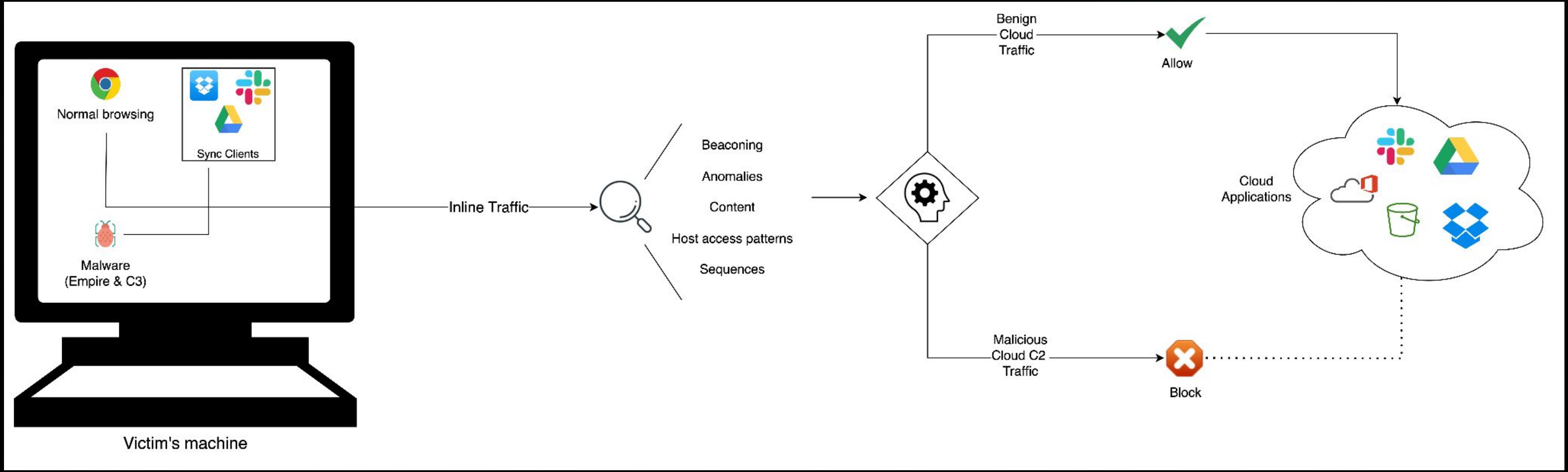
- Combine all of the signals into a POC threshold based test

- In our analysis, we opt for the following:

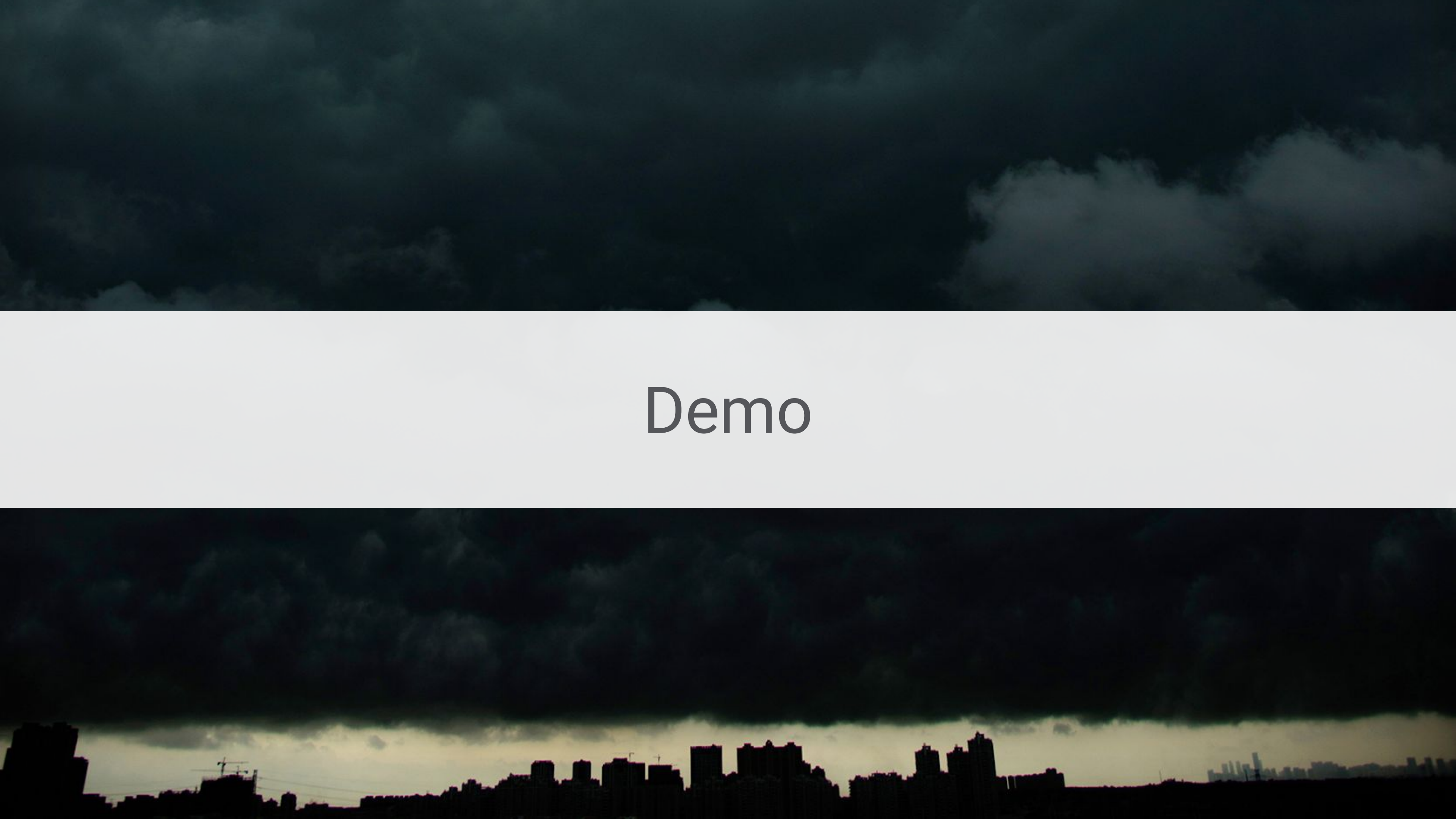
    - If the traffic from one process to one domain contains more than 5 of the indicators, “raise an alert”

- Ideally, we want to use a more robust statistical analysis component (not just an arbitrary magic “5”)

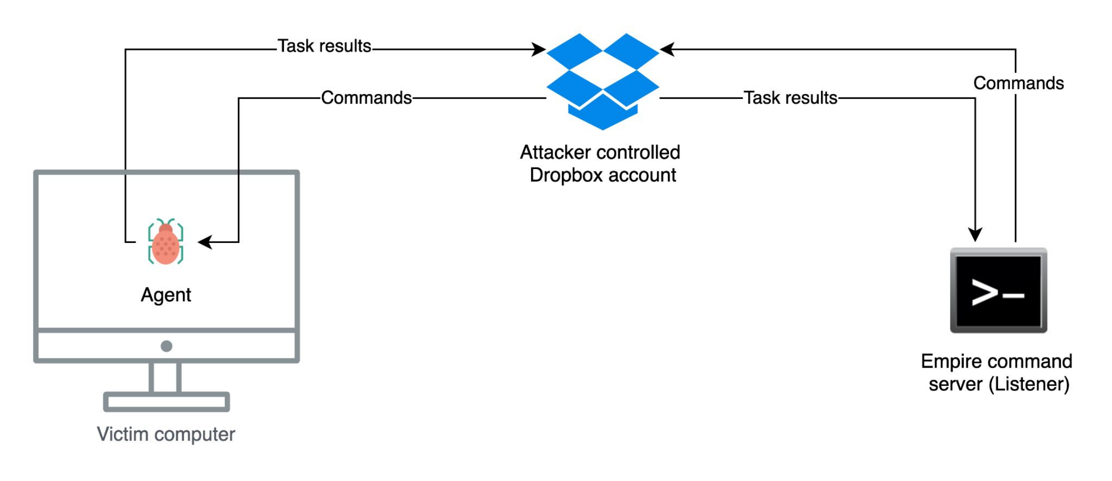
Our Approach (revisited)



Demo

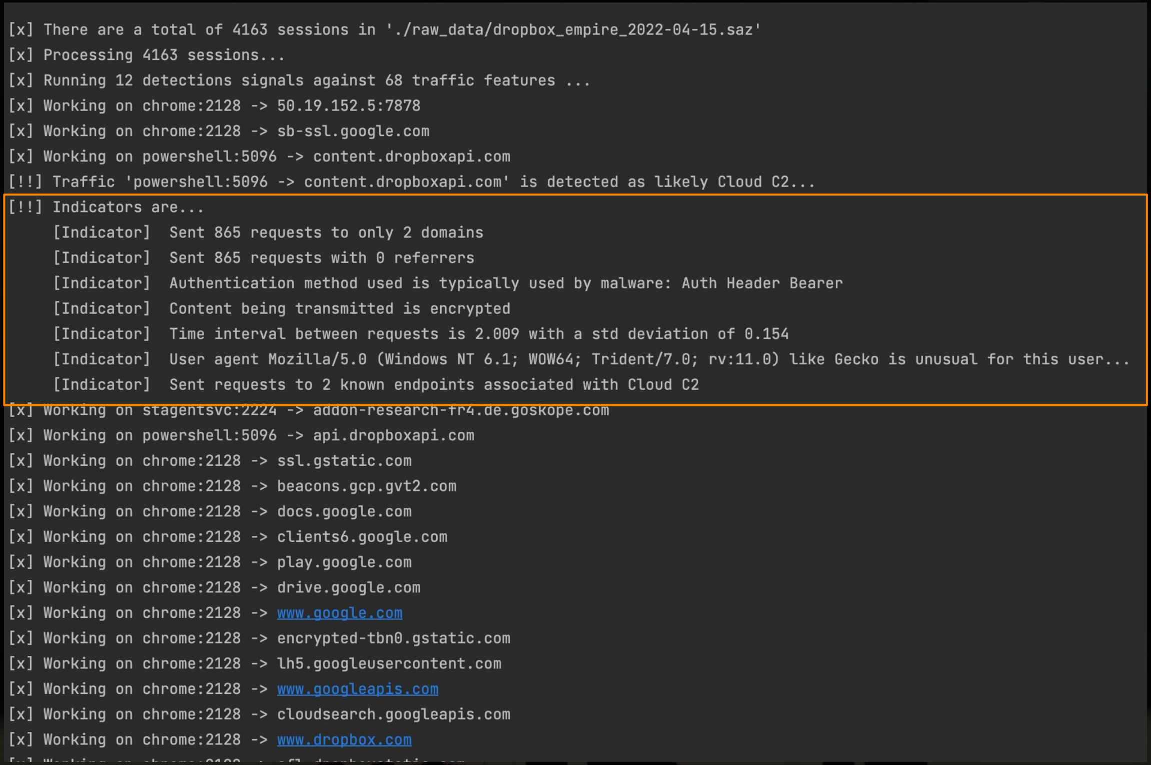


Example 1 - Dropbox + Empire


Task results
Commands
Attacker controlled Dropbox account
Commands
Task results
Agent
Victim computer
>_
Empire command server (Listener)

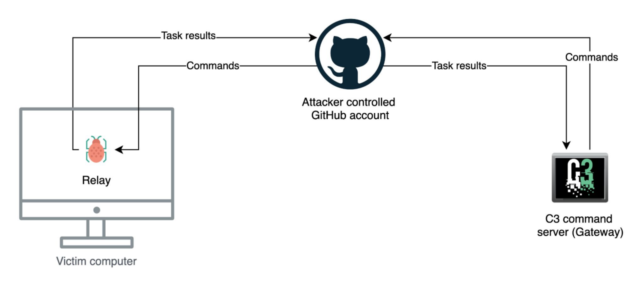
Example 1 - Dropbox + Empire

Example 1 - Dropbox + Empire

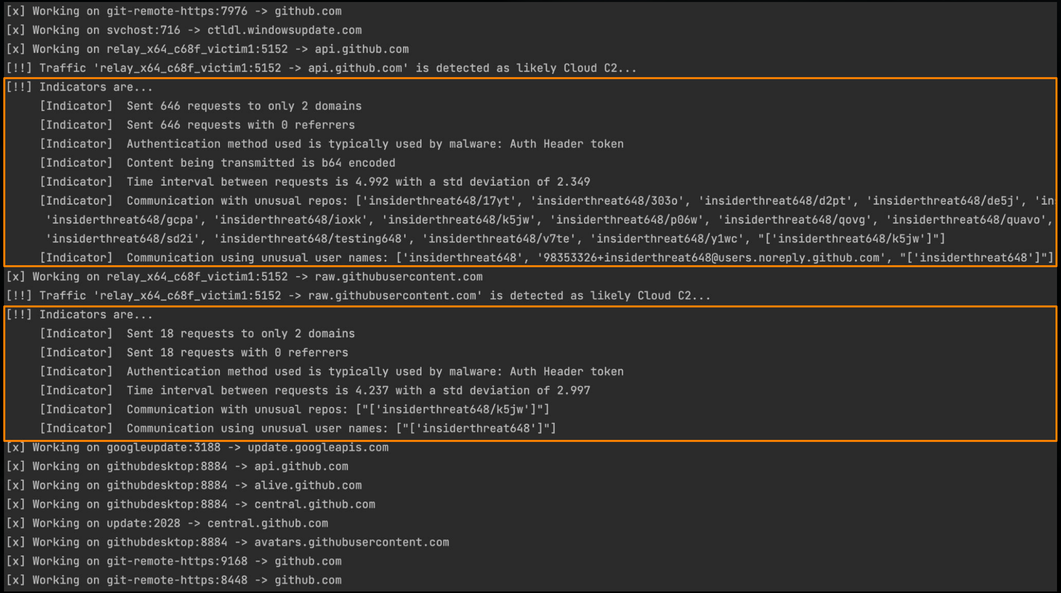


```
[x] There are a total of 4163 sessions in './raw_data/dropbox_empire_2022-04-15.saz'
[x] Processing 4163 sessions...
[x] Running 12 detections signals against 68 traffic features ...
[x] Working on chrome:2128 -> 50.19.152.5:7878
[x] Working on chrome:2128 -> sb-ssl.google.com
[x] Working on powershell:5096 -> content.dropboxapi.com
[!!] Traffic 'powershell:5096 -> content.dropboxapi.com' is detected as likely Cloud C2...
[!!] Indicators are...
     [Indicator]  Sent 865 requests to only 2 domains
     [Indicator]  Sent 865 requests with 0 referrers
     [Indicator]  Authentication method used is typically used by malware: Auth Header Bearer
     [Indicator]  Content being transmitted is encrypted
     [Indicator]  Time interval between requests is 2.009 with a std deviation of 0.154
     [Indicator]  User agent Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko is unusual for this user...
     [Indicator]  Sent requests to 2 known endpoints associated with Cloud C2
[x] Working on stagentsvc:2224 -> addon-research-fr4.de.goskope.com
[x] Working on powershell:5096 -> api.dropboxapi.com
[x] Working on chrome:2128 -> ssl.gstatic.com
[x] Working on chrome:2128 -> beacons.gcp.gvt2.com
[x] Working on chrome:2128 -> docs.google.com
[x] Working on chrome:2128 -> clients6.google.com
[x] Working on chrome:2128 -> play.google.com
[x] Working on chrome:2128 -> drive.google.com
[x] Working on chrome:2128 -> www.google.com
[x] Working on chrome:2128 -> encrypted-tbn0.gstatic.com
[x] Working on chrome:2128 -> lh5.googleusercontent.com
[x] Working on chrome:2128 -> www.googleapis.com
[x] Working on chrome:2128 -> cloudsearch.googleapis.com
[x] Working on chrome:2128 -> www.dropbox.com
[x] Working on chrome:2128 -> cfl.dropboxstatic.com
```

Example 2 - GitHub + C3

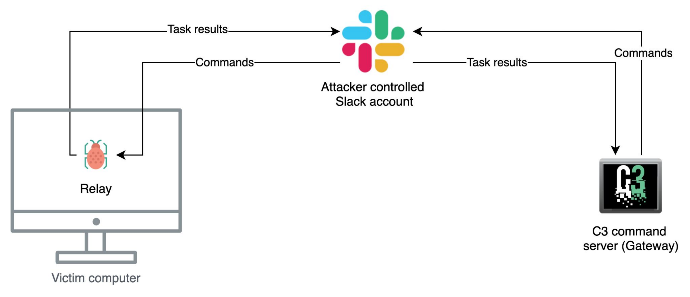


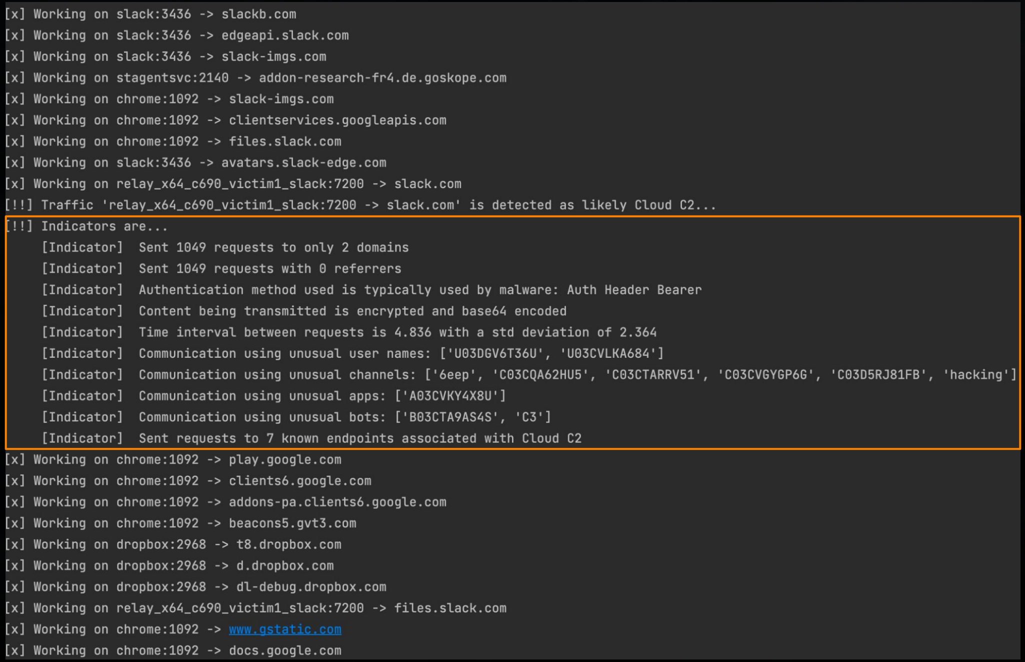
Task results
Commands
Task results
Commands
Attacker controlled GitHub account
Relay
C3 command server (Gateway)
Victim computer



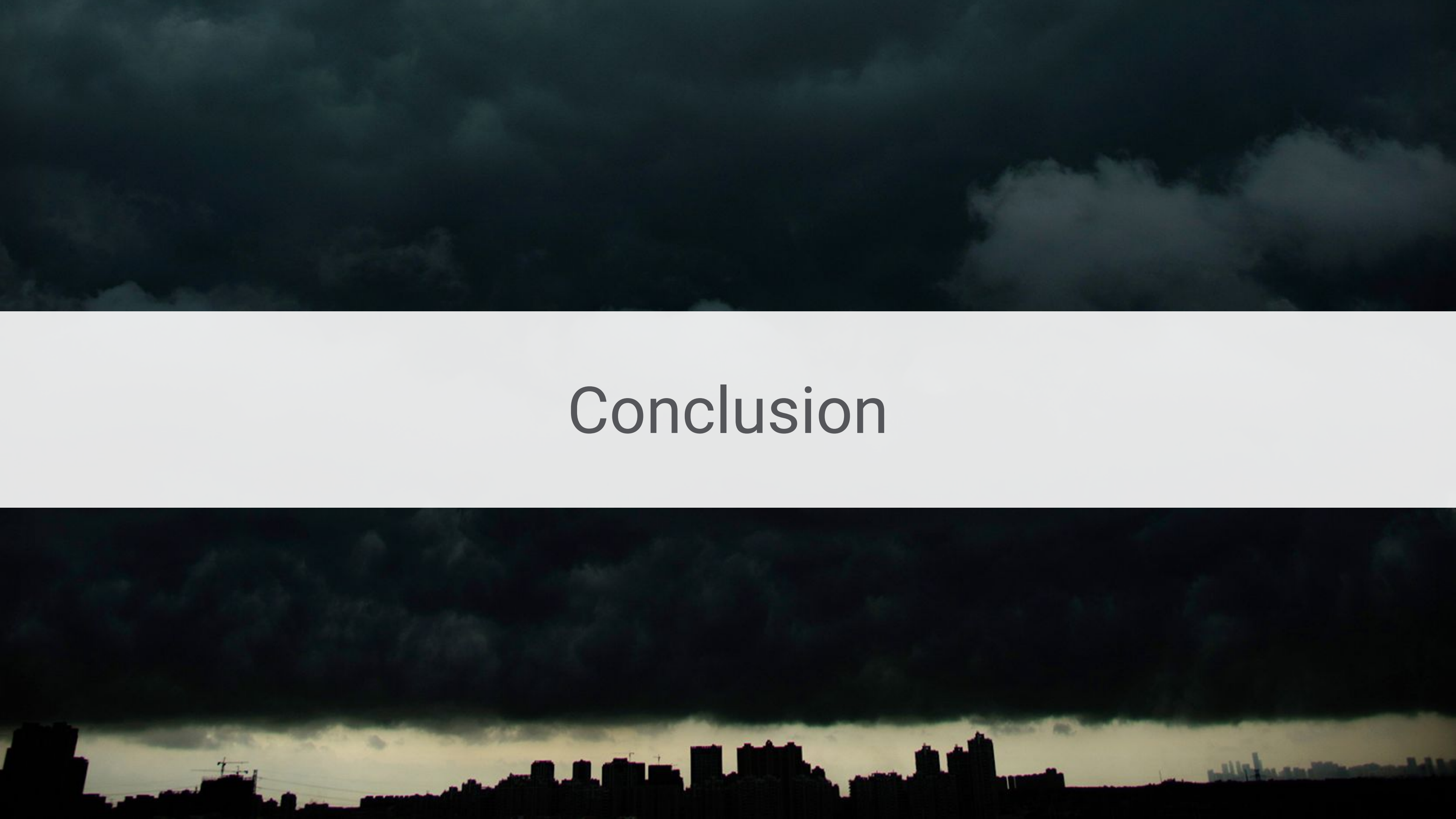
```
[x] Working on git-remote-https:7976 -> github.com
[x] Working on svchost:716 -> ctldl.windowsupdate.com
[x] Working on relay_x64_c68f_victim1:5152 -> api.github.com
[!!] Traffic 'relay_x64_c68f_victim1:5152 -> api.github.com' is detected as likely Cloud C2...
[!!] Indicators are...
     [Indicator]  Sent 646 requests to only 2 domains
     [Indicator]  Sent 646 requests with 0 referrers
     [Indicator]  Authentication method used is typically used by malware: Auth Header token
     [Indicator]  Content being transmitted is b64 encoded
     [Indicator]  Time interval between requests is 4.992 with a std deviation of 2.349
     [Indicator]  Communication with unusual repos: ['insiderthreat648/17yt', 'insiderthreat648/303o', 'insiderthreat648/d2pt', 'insiderthreat648/de5j', 'in
      'insiderthreat648/gcpa', 'insiderthreat648/ioxk', 'insiderthreat648/k5jw', 'insiderthreat648/p06w', 'insiderthreat648/qovg', 'insiderthreat648/quavo',
      'insiderthreat648/sd2i', 'insiderthreat648/testing648', 'insiderthreat648/v7te', 'insiderthreat648/y1wc', "['insiderthreat648/k5jw']"]
     [Indicator]  Communication using unusual user names: ['insiderthreat648', '98353326+insiderthreat648@users.noreply.github.com', "['insiderthreat648']"]
[x] Working on relay_x64_c68f_victim1:5152 -> raw.githubusercontent.com
[!!] Traffic 'relay_x64_c68f_victim1:5152 -> raw.githubusercontent.com' is detected as likely Cloud C2...
[!!] Indicators are...
     [Indicator]  Sent 18 requests to only 2 domains
     [Indicator]  Sent 18 requests with 0 referrers
     [Indicator]  Authentication method used is typically used by malware: Auth Header token
     [Indicator]  Time interval between requests is 4.237 with a std deviation of 2.997
     [Indicator]  Communication with unusual repos: ["['insiderthreat648/k5jw']"]
     [Indicator]  Communication using unusual user names: ["['insiderthreat648']"]
[x] Working on googleupdate:3188 -> update.googleapis.com
[x] Working on githubdesktop:8884 -> api.github.com
[x] Working on githubdesktop:8884 -> alive.github.com
[x] Working on githubdesktop:8884 -> central.github.com
[x] Working on update:2028 -> central.github.com
[x] Working on githubdesktop:8884 -> avatars.githubusercontent.com
[x] Working on git-remote-https:9168 -> github.com
[x] Working on git-remote-https:8448 -> github.com
```

Example 3 - Slack + C3





```
[x] Working on slack:3436 -> slackb.com
[x] Working on slack:3436 -> edgeapi.slack.com
[x] Working on slack:3436 -> slack-imgs.com
[x] Working on stagentsvc:2140 -> addon-research-fr4.de.goskope.com
[x] Working on chrome:1092 -> slack-imgs.com
[x] Working on chrome:1092 -> clientservices.googleapis.com
[x] Working on chrome:1092 -> files.slack.com
[x] Working on slack:3436 -> avatars.slack-edge.com
[x] Working on relay_x64_c690_victim1_slack:7200 -> slack.com
[!!] Traffic 'relay_x64_c690_victim1_slack:7200 -> slack.com' is detected as likely Cloud C2...
[!!] Indicators are...
     [Indicator]  Sent 1049 requests to only 2 domains
     [Indicator]  Sent 1049 requests with 0 referrers
     [Indicator]  Authentication method used is typically used by malware: Auth Header Bearer
     [Indicator]  Content being transmitted is encrypted and base64 encoded
     [Indicator]  Time interval between requests is 4.836 with a std deviation of 2.364
     [Indicator]  Communication using unusual user names: ['U03DGV6T36U', 'U03CVLKA684']
     [Indicator]  Communication using unusual channels: ['6eep', 'C03CQA62HU5', 'C03CTARRV51', 'C03CVGYGP6G', 'C03D5RJ81FB', 'hacking']
     [Indicator]  Communication using unusual apps: ['A03CVKY4X8U']
     [Indicator]  Communication using unusual bots: ['B03CTA9AS4S', 'C3']
     [Indicator]  Sent requests to 7 known endpoints associated with Cloud C2
[x] Working on chrome:1092 -> play.google.com
[x] Working on chrome:1092 -> clients6.google.com
[x] Working on chrome:1092 -> addons-pa.clients6.google.com
[x] Working on chrome:1092 -> beacons5.gvt3.com
[x] Working on dropbox:2968 -> t8.dropbox.com
[x] Working on dropbox:2968 -> d.dropbox.com
[x] Working on dropbox:2968 -> dl-debug.dropbox.com
[x] Working on relay_x64_c690_victim1_slack:7200 -> files.slack.com
[x] Working on chrome:1092 -> www.gstatic.com
[x] Working on chrome:1092 -> docs.google.com
```



Conclusion

Conclusion

- What is Cloud C2? *Command and Control via a Cloud Application*
- Why is Cloud C2 hard to detect? *C2 traffic is going to a valid cloud provider’s server*
- Detection approach *Used a set of behaviour signals to identify Cloud C2*
- Demonstration *Can quickly write some tooling to use the signals discussed*

Contact

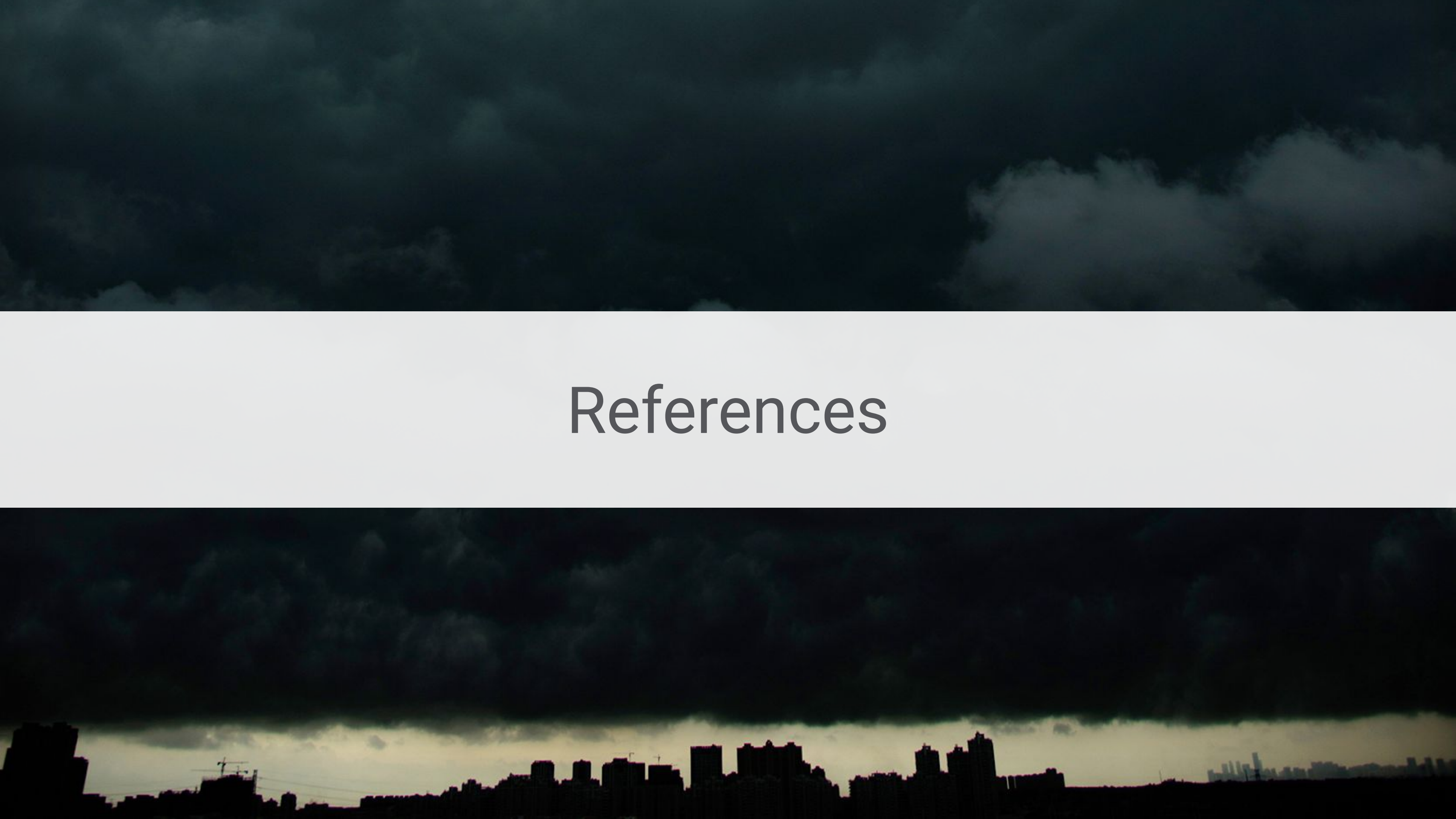
Twitter: @dagmulu

Linkedin: dmulugeta

Future updates on our Netskope Threat Labs Blog

Danke!

Questions?



References

References

[1] https://labs.f-secure.com/blog/hunting-for-c3/

[2] https://www.f-secure.com/gb-en/consulting/our-thinking/rip-office365-command-and-control

[3] https://labs.f-secure.com/tools/c3

[4] https://attack.mitre.org/techniques/T1102/002/

[5] https://attack.mitre.org/techniques/T1102/

[6] https://labs.f-secure.com/blog/attack-detection-fundamentals-c2-and-exfiltration-lab-1

[7] https://labs.f-secure.com/blog/attack-detection-fundamentals-c2-and-exfiltration-lab-2

[8] https://labs.f-secure.com/blog/attack-detection-fundamentals-c2-and-exfiltration-lab-3

[9] https://sansorg.egnyte.com/dl/4mdnX7hSOV

[10] https://securityintelligence.com/how-to-leverage-log-services-to-analyze-cc-traffic/

[11] https://cybersecurity.att.com/blogs/security-essentials/command-and-control-server-detection-methods-best-practices

[12] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

[13] https://blog.bushidotoken.net/2021/04/dead-drop-resolvers-espionage-inspired.htmll

[14] https://www.bleepingcomputer.com/news/security/state-sponsored-hackers-abuse-slack-api-to-steal-airline-data/

[15] https://thehackernews.com/2022/01/molerats-hackers-hiding-new-espionage.html

[16] https://thehackernews.com/2022/01/hackers-exploited-mshtml-flaw-to-spy-on.html

[17] https://www.trendmicro.com/en_us/research/20/l/pawn-storm-lack-of-sophistication-as-a-strategy.html

[18] https://github.com/Coalfire-Research/Slackor

[19] https://github.com/praetorian-inc/slack-c2bot

[20] https://github.com/bkup/SlackShell

[21] https://github.com/Arno0x/DBC2

[22] https://github.com/FSecureLABS/C3

[23] https://github.com/3xpl01tc0d3r/Callidus

[24] https://github.com/boku7/azureOutlookC2

[25] https://github.com/looCiprian/GC2-sheet

[26] https://github.com/BC-SECURITY

[27] https://github.com/BC-SECURITY/Empire

[28] https://www.bc-security.org/post/empire-dropbox-c2-listener/

[29] https://aws.amazon.com/workspaces/

Future improvements

- More data analysis…
- TBD