



Threat Intel Report

Cal Poly Pomona FAST (DFIR Research Team)

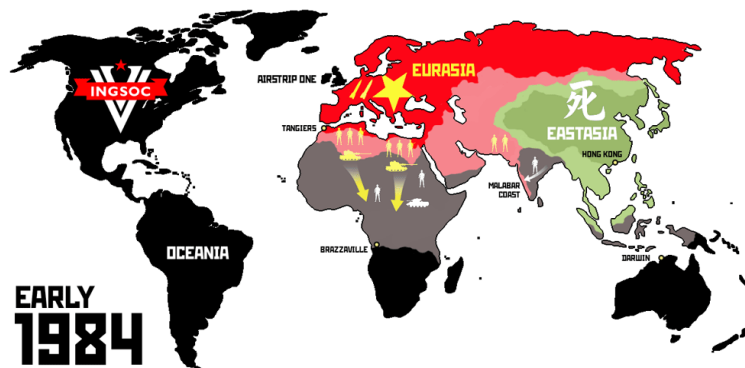
Introduction:

FAST's DFIR branch works with major cloud computing platforms as auxiliary security contractors with a specialization in Detection and Response. While we occasionally work with Junglebook and Gargoyle, our primary workload consists of incident response for the Asura Megacorp and its clients. We work on classified incidents to improve global stability and overall security posture.

Executive Summary:

- New Atlantean APT detected. Dubbed 'Aquarius' this group was discovered to have been actively engaged in cyber attacks against MSPs and MSSPs providing digital services to a select subset of infrastructure companies.
- The targets' primary business models focus on laying undersea communication and fiber optic cables that connect Oceania, Eurasia & Eastasia.
- Motives seem to relate to perceived interference with local oceanic life and potential resurgence of ideologically motivated Atlantean militia groups.
- Impact ranges from moderate to severe.
- Persistent activity spotted throughout three primary regions.

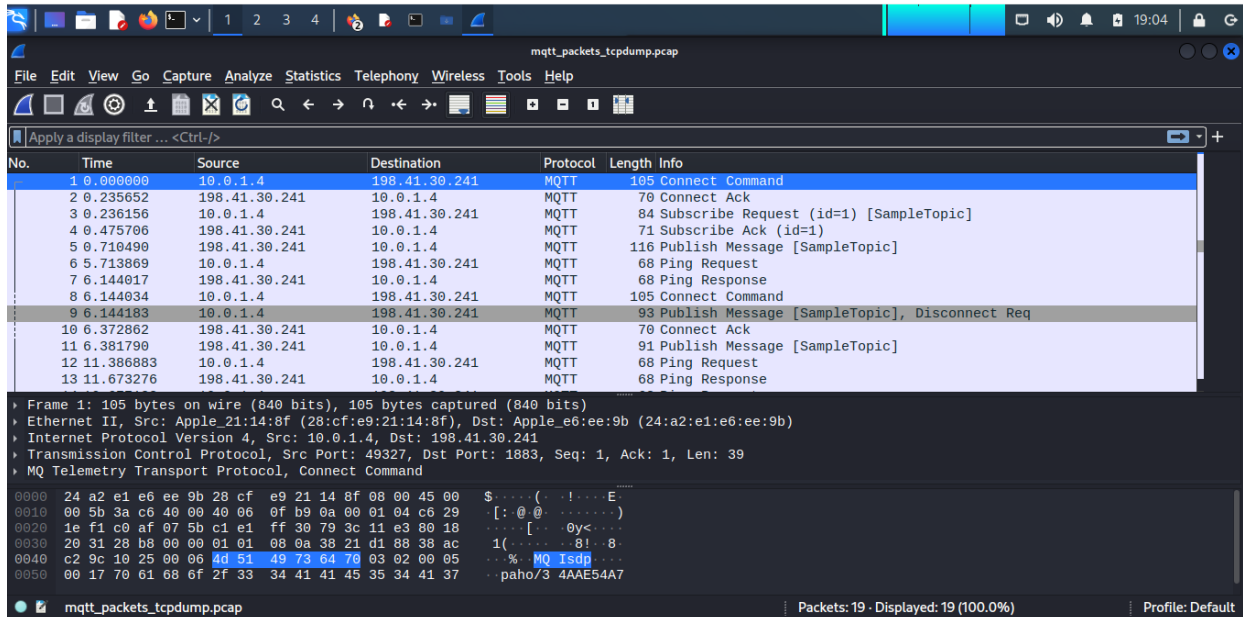
Threat Map:



- Regions affected:
 - 1) MSPs supporting the Pacific region between Oceania and Eastasia
 - 2) MSPs supporting the Atlantic region between Oceania to Eurasia
 - 3) MSSPs providing cybersecurity services to undersea cable companies in all three superstates.

Threat Detail:

Our Investigation has discovered a data poisoning supply chain attack via Lyquidity Co.'s Leviathan software, an underwater infrastructure health monitoring and reporting tool that sends data from underwater sensors to their respective organization's data collection infrastructure silos across different MSPs serving underwater infrastructure companies.



The image shows a Wireshark packet capture of MQTT traffic. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.1.4	198.41.30.241	MQTT	105	Connect Command
2	0.235652	198.41.30.241	10.0.1.4	MQTT	70	Connect Ack
3	0.236156	10.0.1.4	198.41.30.241	MQTT	84	Subscribe Request (id=1) [SampleTopic]
4	0.475706	198.41.30.241	10.0.1.4	MQTT	71	Subscribe Ack (id=1)
5	0.710490	198.41.30.241	10.0.1.4	MQTT	116	Publish Message [SampleTopic]
6	5.713869	10.0.1.4	198.41.30.241	MQTT	68	Ping Request
7	6.144617	198.41.30.241	10.0.1.4	MQTT	68	Ping Response
8	6.144634	10.0.1.4	198.41.30.241	MQTT	105	Connect Command
9	6.144183	10.0.1.4	198.41.30.241	MQTT	93	Publish Message [SampleTopic], Disconnect Req
10	6.372862	198.41.30.241	10.0.1.4	MQTT	70	Connect Ack
11	6.381790	198.41.30.241	10.0.1.4	MQTT	91	Publish Message [SampleTopic]
12	11.386883	10.0.1.4	198.41.30.241	MQTT	68	Ping Request
13	11.673276	198.41.30.241	10.0.1.4	MQTT	68	Ping Response

The packet details pane for Frame 1 (MQTT Connect Command) shows the following information:

- Frame 1: 105 bytes on wire (840 bits), 105 bytes captured (840 bits)
- Ethernet II, Src: Apple_21:14:8f (28:cf:e9:21:14:8f), Dst: Apple_e6:ee:9b (24:a2:e1:e6:ee:9b)
- Internet Protocol Version 4, Src: 10.0.1.4, Dst: 198.41.30.241
- Transmission Control Protocol, Src Port: 49327, Dst Port: 1883, Seq: 1, Ack: 1, Len: 39
- MQ Telemetry Transport Protocol, Connect Command

The packet bytes pane shows the raw data in hexadecimal and ASCII. The ASCII column shows the MQTT protocol header and payload, including the topic 'SampleTopic' and the message 'MQ Isdp'.

Poisoned Data Stream

IoT Hub - Anomalous Activity Detected

From azure-notification <azure-notification@proton.me>

To elk-senior-dev@proton.me

Date Friday, December 2nd, 2022 at 6:31 AM



Dear User,

Our records have detected anomalous activity from your IoT sensors tied to the us-east data center. Please download the attachment below for the full report.

Azure Data Team



[Privacy Statement](#)

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052



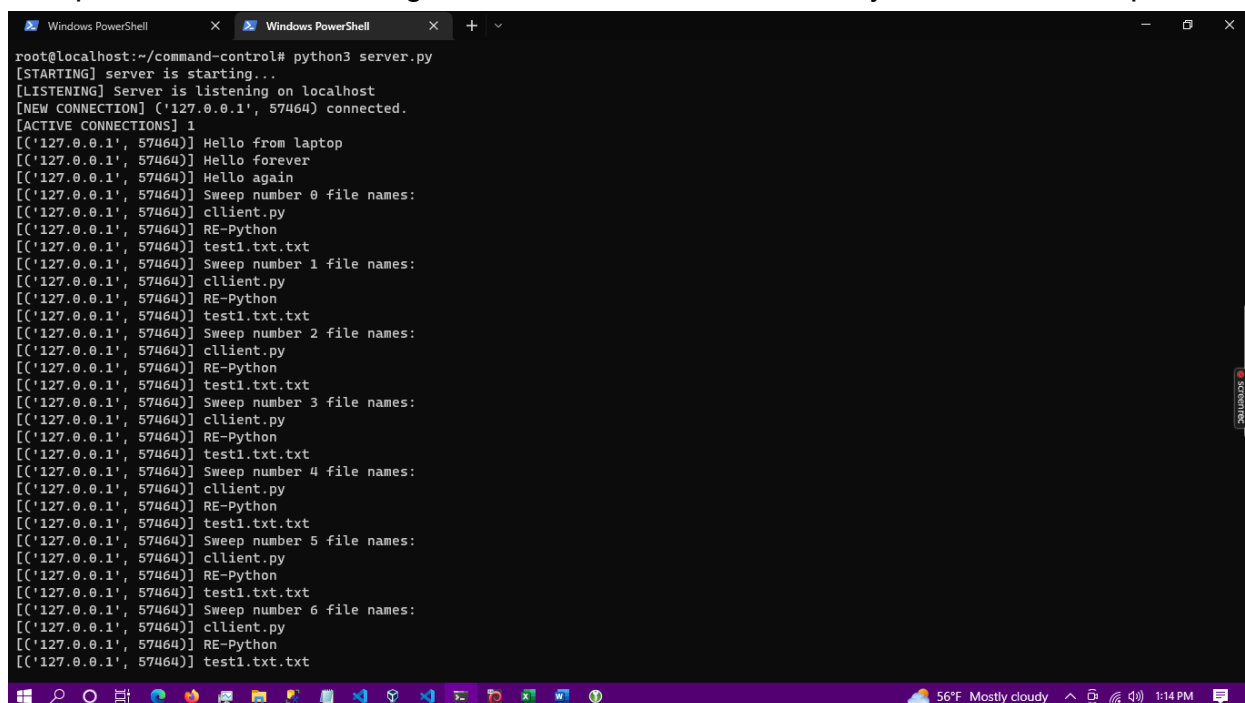
230.48 KB 1 file attached 1 embedded image

incident-report.pdf.py 1.28 KB

Azure Phishing Email

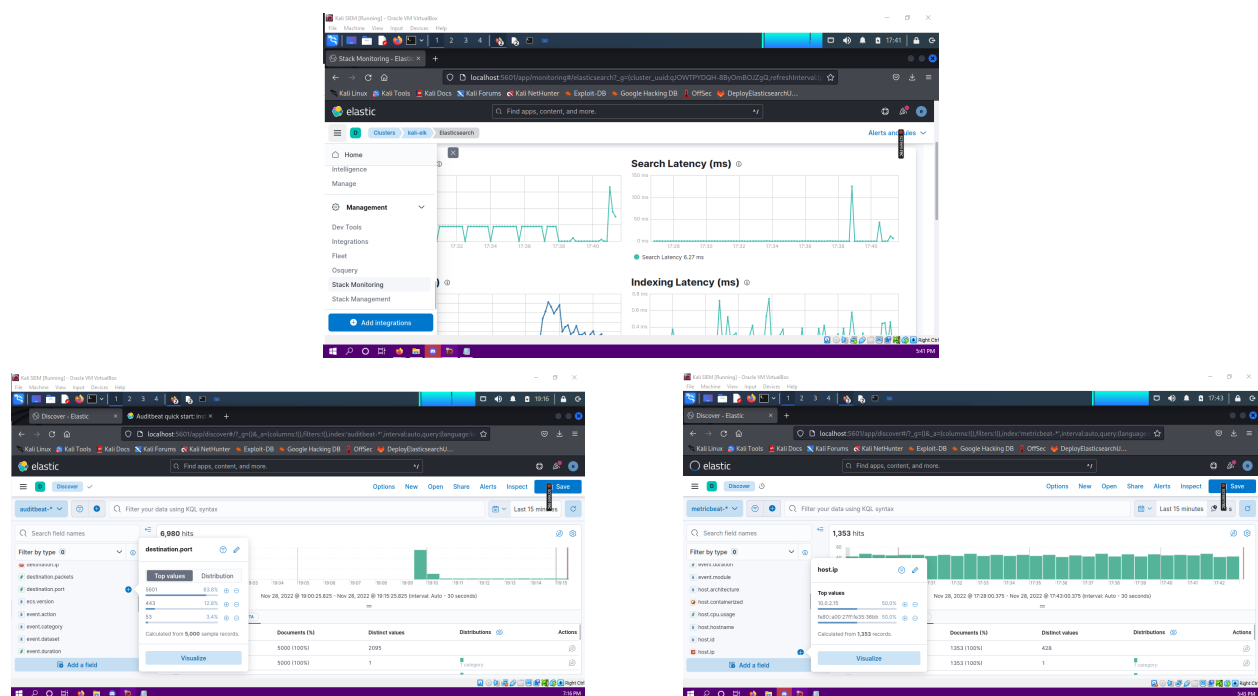
The attack on the MSPs in question seems to have intentionally triggered the software's emergency response protocol wherein temporary measures were taken to automatically notify their respective customers. These notices, sent to and from nearby cloud data centers were intercepted on their way from the IoT Hub Cloud provider to the customers. The MiTM attack has redistributed the msg with malicious attachments containing malware beacons.

Despite obfuscation attempts, FAST's DFIR Research Team detected 3 interrelated attacks with the help of custom ELK SIEM. Upon infection, malware beacons established websocket connections to an IPv4 address linked to a command and control server. The attackers were able to harvest sensitive user and client data and then pivot their attacks to target the MSPs and MSSPs directly via a malicious update.



```
Windows PowerShell X Windows PowerShell X + -
root@localhost:~/command-control# python3 server.py
[STARTING] server is starting...
[LISTENING] Server is listening on localhost
[NEW CONNECTION] ('127.0.0.1', 57464) connected.
[ACTIVE CONNECTIONS] 1
[('127.0.0.1', 57464)] Hello from laptop
[('127.0.0.1', 57464)] Hello forever
[('127.0.0.1', 57464)] Hello again
[('127.0.0.1', 57464)] Sweep number 0 file names:
[('127.0.0.1', 57464)] cllient.py
[('127.0.0.1', 57464)] RE-Python
[('127.0.0.1', 57464)] test1.txt.txt
[('127.0.0.1', 57464)] Sweep number 1 file names:
[('127.0.0.1', 57464)] cllient.py
[('127.0.0.1', 57464)] RE-Python
[('127.0.0.1', 57464)] test1.txt.txt
[('127.0.0.1', 57464)] Sweep number 2 file names:
[('127.0.0.1', 57464)] cllient.py
[('127.0.0.1', 57464)] RE-Python
[('127.0.0.1', 57464)] test1.txt.txt
[('127.0.0.1', 57464)] Sweep number 3 file names:
[('127.0.0.1', 57464)] cllient.py
[('127.0.0.1', 57464)] RE-Python
[('127.0.0.1', 57464)] test1.txt.txt
[('127.0.0.1', 57464)] Sweep number 4 file names:
[('127.0.0.1', 57464)] cllient.py
[('127.0.0.1', 57464)] RE-Python
[('127.0.0.1', 57464)] test1.txt.txt
[('127.0.0.1', 57464)] Sweep number 5 file names:
[('127.0.0.1', 57464)] cllient.py
[('127.0.0.1', 57464)] RE-Python
[('127.0.0.1', 57464)] test1.txt.txt
[('127.0.0.1', 57464)] Sweep number 6 file names:
[('127.0.0.1', 57464)] cllient.py
[('127.0.0.1', 57464)] RE-Python
[('127.0.0.1', 57464)] test1.txt.txt
```

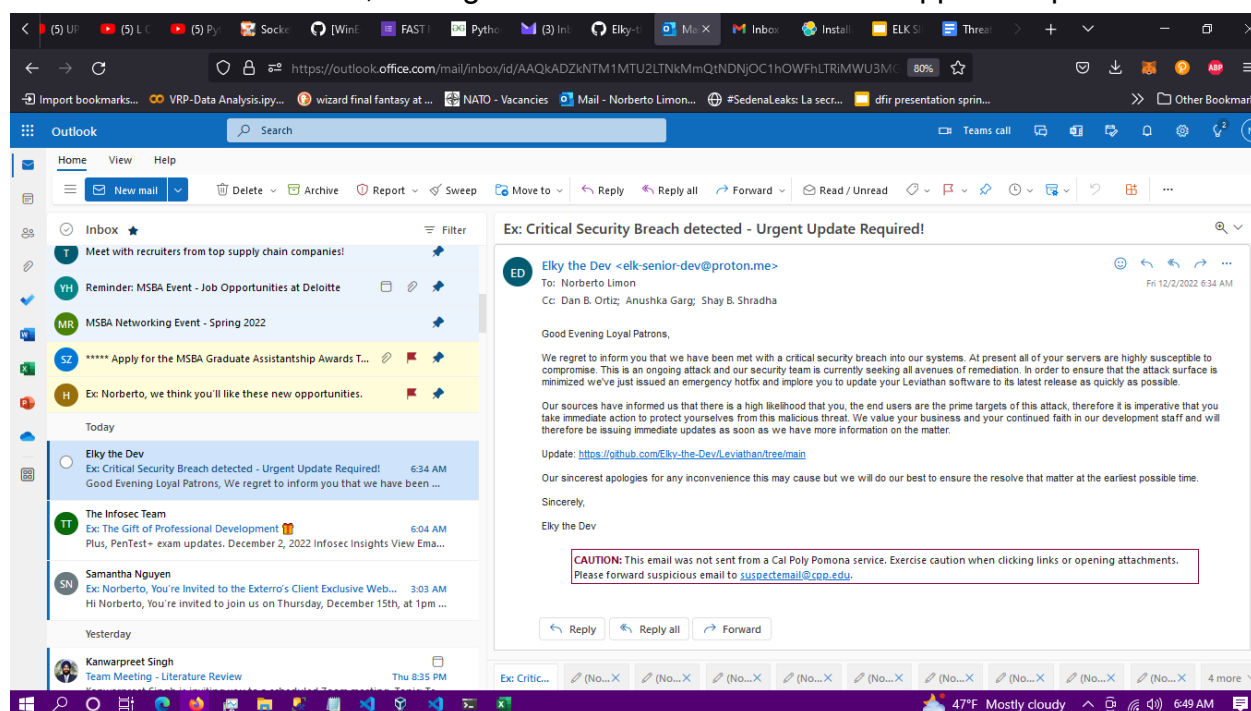
Beacon data extraction



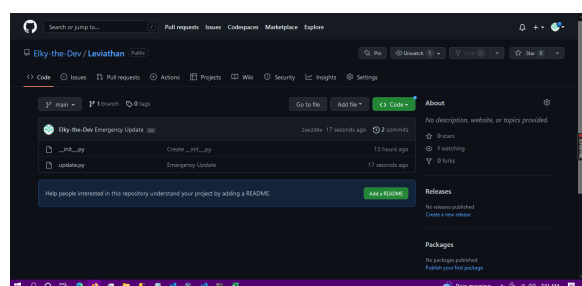
Elasticsearch data & indices relevant to our dashboard assembly

We believe these beacons were being used to gather information that would inform the attackers of strategically important targets which would be prime candidates for a follow-up spearfishing ransomware attack. Through the confusion over the data poisoning attack remediation, the targets were particularly susceptible to opening attachments that offered suggestions for remediation from upper management. With the information gathered by the beacons, it is likely that the attackers used this newly gathered intel to deploy ransomware that would cause damage both to the Infrastructure companies and to Lyquidity Co's reputation as the most reliable organization of its kind well as the functionality of its many MSP and MSSP affiliates that depend on them.

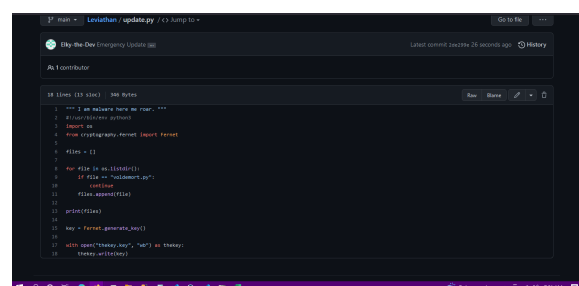
The follow up ransomware attack was introduced via changes to the supply chain infrastructure code (via GitHub using credentials of a senior developer at Lyquidity) and was deployed against MSSPs monitoring the Leviathan Software backend as well as the local infrastructure of the companies that used Leviathan when they updated the Leviathan Client software, turning it into ransomware after the supposed update.



Email msg asking users to install malicious update via GitHub



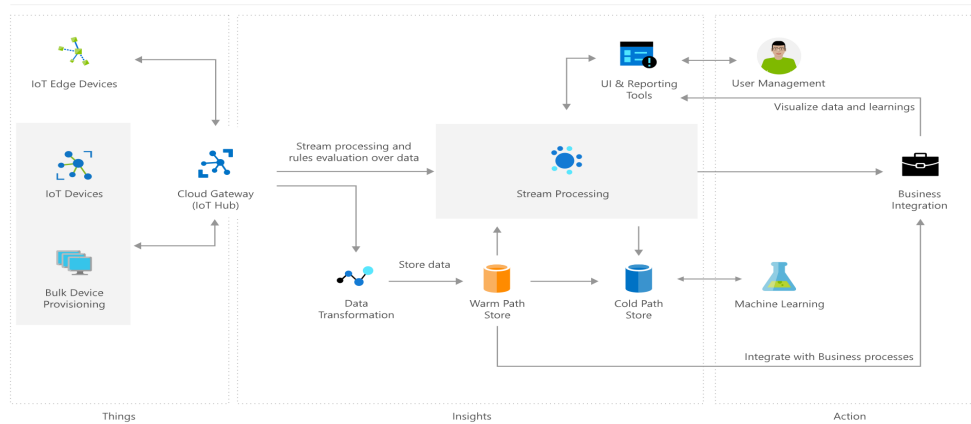
GitHub update containing malicious payload



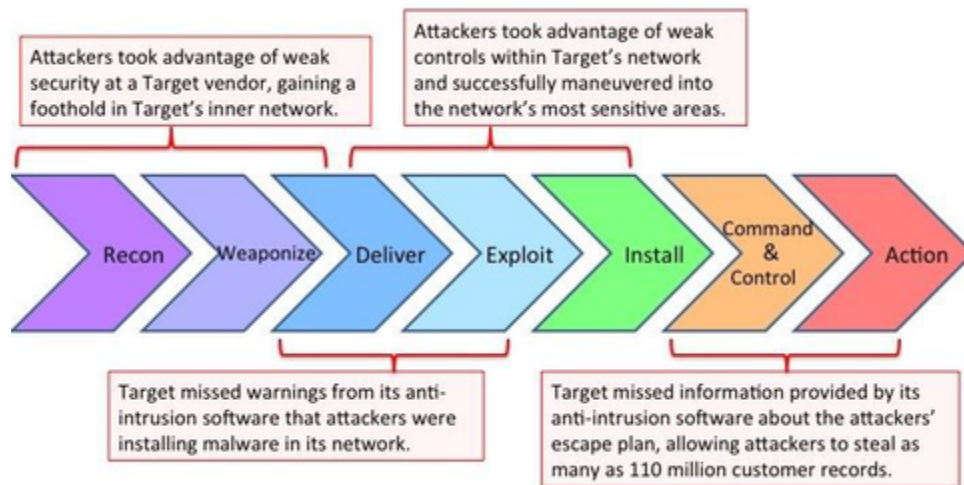
Ransomware Malware file and code

The attack was stopped before this update was deployed. We may have reason to believe that this email approach was not the initially intended avenue of attack which if successful would have infected every client and affiliate of Lyquidity Co.

External Architecture Layout:



Cyber Kill Chain:



- > Reconnaissance
- > Weaponization
- > Delivery
- > Exploitation
- > Installation
- > Command & Control
- > Subsequent Actions

Attack Sequence:

Phase 1: Sensors to Cloud (Recon / Weaponization / Delivery)

- IoT Sensors are compromised.
- Begin issuing inaccurate data streams
- Emergency response triggered in Cloud infrastructure

☑ {Data Poisoned} [First Attack]

IoT Sensors -> IoT Hub -> Data Stream (Lambda Architecture):

1) Cloud Pipeline -> Data Transformation -> Internal Logic

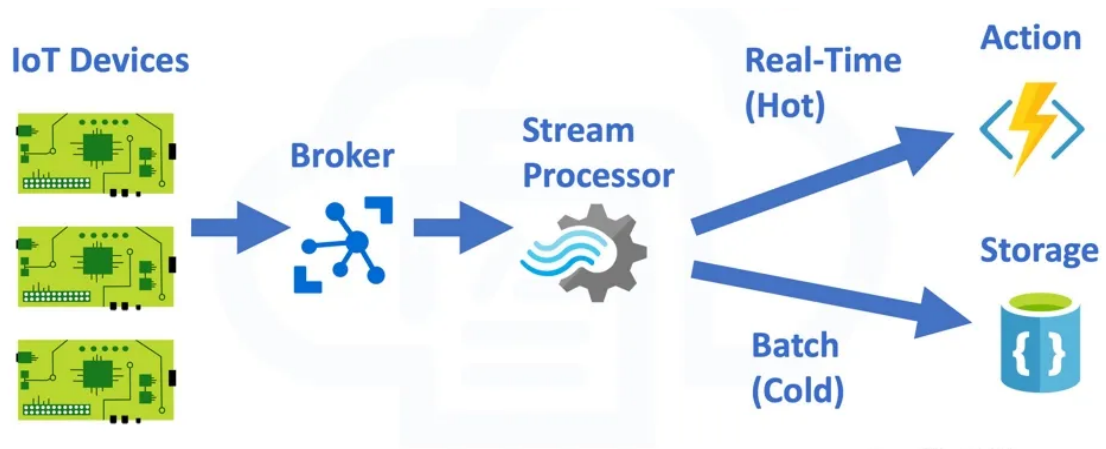
Phase 2: Cloud to Offline (Delivery / Exploit / Install)

- Cloud Infrastructure sends notice to senior dev.
- Notice intercepted. Retransmitted with malicious payload
- Attachment opened, payload installed.
- Malware beacon gathers and sends sensitive data to C2 Server

2) Offline Pipeline -> MiTM -> dev infrastructure -> credentials + client list acquired

☑ {Beacon/Recon} [Second Attack]

Lambda Component:



<https://Build5Nines.com>

(1) = Cloud Pipeline = Real Time Pipeline = Hot Pipeline




(2) = Offline Pipeline = Batch Pipeline = Cold Pipeline

Phase 3: Offline to Client Update (Command & Control / Actions)

According to Threat Intel provided by other groups doing similar work:

- Using stolen credentials, C2 emails clients to install an update containing ransomware.
- Ransomware is deployed on client infrastructure.
- Client systems locked

Fake email -> GitHub Update -> clients [devs + customers]

 {Ransomware} [3rd Attack]  

Remediation Steps:

Using ELK we were able to detect malicious activity coming to and from the offline component of the backend:

1. MiTM attack w/ tampered email notice containing undetected malware beacon arrives on scene
2. Malicious activity detected in Download's folder with auditd and AuditBeat and Packetbeat
3. Correlation made with Packetbeat, Metricbeat and open source threat intel; malware beacon discovered
4. Irregular github login activity from senior dev on vacation detected with Auditbeat and Logstash's GitHub plugin
5. Ransomware discovered; Notified Juniper; Full Stop. Reverse Engineering of pending update ongoing

Suggestions:

We suggest that senior officials immediately make a public announcement in addition to phone contact with client companies' top security personnel to ensure your clients are able to distinguish between the false update notice and the real notice telling them not to install the update. Lyquidity's CISO should reach out to and coordinate with other organizations trying to remedy this issue ASAP. We would recommend prioritizing the removal of the beacon malware after the ransomware attack surface has been minimized and then immediate removal of the two pieces of malware as well as an investigation into the data poisoning attack that triggered the timely warning that was swapped during the MiTM attack.

Exploit Inventory:

Malicious Files	Description	Status
incident-report.pdf.py	Malware beacon	Contained ▾
pdf.py	Trojan pdf packaged with malware beacon	Contained ▾
update.py	Malicious update [Ransomware]	In progress ▾
Data Injection	Data Poisoning Attack	Under review ▾

Conclusions:

This particular ransomware attack had some notable features that distinguish it from other ransomware attacks. First, it repurposed existing software that was integral to the core functionality of its clients and affiliates and turned that core functionality into core dysfunctionality. Second, it did not ask for financial compensation and did not offer a means of decryption. This seemed to have been intended to maximize damage output.