The VoIP PBX Honeypot Advance Persistent Threat Analysis

N. Mcinnes and G. Wills

Department of Electronics and Computer Science, Faculty of Engineering and Physical Sciences,
University of Southampton, U.K.

Keywords: VoIP, SIP, PBX Hacking, IRSF, Toll Fraud, APT, Next Generation Networks.

Abstract: PBX hacking is a multi-billion dollar per year criminal and terrorism funding source. This paper follows on from a previous 10-day Honeypot experiment, to run a VoIP PBX Honeypot for a longer period of 103-day to not only validate any similarities, but to also analyse non-VoIP methods hackers use in an attempt to gain access to a VoIP System. Over the 103-day data collection period, the Honeypot recorded over 100 million SIP messages. Different techniques were used (including SQL injections in Invites) and hackers of the same IP subnet also attempted using web vulnerabilities in different telephony phone systems to gain access. Of specific interest, over the Christmas period of 2018, attack intensity decreased significantly. To validate these findings, the Honeypot experiment was also conducted for a short period over the Christmas period of 2019 which found that unlike Christmas 2018, attacks increased. The sophistication, scale and complexity of the fraud would suggest an Advance Persistent Threat exists with an aim to infiltrate a VoIP system (including a PBX) to conduct Toll Fraud and where possible to also add that system to a botnet of infected voice systems.

1 INTRODUCTION

Telephone networks are currently migrating from Time-Division Multiplexing (TDM) networks to Voice over Internet Protocol (VoIP) using Next Generation Networking (NGN) technologies using the IP Telephony protocol Session Initiated Protocol (SIP) (Colin and Richard, 2019), (Ofcom, 2007). This transition will allow organisations (both the communications operator and end organisation) to reduce costs and increase flexibility[1] [2]. The United Kingdom is an example where this is due to be completed by 2025 (Colin and Richard, 2019). Therefore, as more organisations move to VoIP and NGNs, it is prudent that the risks are carefully examined. Especially as large phone bills can be caused in a short period of time, documented in some cases to be in excess of $100,000 (New York Times, 2014), (Central Netherlands District Court, 2014).

A Private Branch Exchange (PBX) is a business phone system which typically connects to their provider through various technologies such as traditional analogue, ISDN or more commonly VoIP which enables calls to the Public Switch Telephone Network (PSTN) enabling a business greater control of their unified communications solutions (Colin and Richard, 2019)[3].

Telephony fraud is a multi-billion-dollar problem (Europol and Trend Micro, 2018). Toll Fraud, also known as International Revenue Share Fraud (enabled via PBX hacking or similar[4]) according to the CFCA is thought to account for approximately 7 billion USD in 2015. It is growing (Marketwired, 2016) and in 2017 was thought to be over 10 billion USD (Privsec Report, 2017). The true costs are still unknown as operators are not necessarily forthcoming due to fear of reputational damage, additional regulation and costs for them and their customers (Europol and Trend Micro, 2018).

Unlike other kinds of frauds, this would affect the customer more than the communications provider as the communications provider would potentially profit from this activity.

A 10-day PBX Honeypot was originally ran that solely focused on VoIP ports (McInnes et al., 2019) to compare to previous historic research conducted. It

[1] https://www.itu.int/en/ITU-T/studygroups/2013-2016/03/Documents/201405-miniworkshop/05-Chaesub-Lee.pdf

[2] https://www.cisco.com/c/dam/en/us/solutions/collateral/executive-perspectives/executive-perspectives/ngn-cio.pdf

[3] https://www.3cx.com/pbx/pbx-phone-system/

[4] https://www.twilio.com/learn/voice-and-video/toll-fraud

Mcinnes, N. and Wills, G.
The VoIP PBX Honeypot Advance Persistent Threat Analysis.
DOI: 10.5220/0010443500700080
In *Proceedings of the 6th International Conference on Internet of Things, Big Data and Security (IoTBDS 2021)*, pages 70-80
ISBN: 978-989-758-504-3

found that attacks were larger (30 time increase from historic Honeypots conducted), more distributed and suggested a botnet of compromised devices. That research focused only on SIP monitoring and the time duration period was limited to 10 days.

To further advance understanding of PBX Hacking, this paper builds off the previous research to run for a longer time duration (115-days – 103-days of data collected) and open up the PBX web ports. This was conducted to see if any new additional behaviour was noticed during a longer time period and to validate the 10-day Honeypot findings. Opening web ports would also determine whether web attacking is conducted as an alternative vector in attempting to break into a PBX.

2 BACKGROUND LITERATURE

2.1 SIP and PBX Overview

Session initiated Protocol (SIP), known by IETF RFC3261 (Internet Engineering Task Force, 2002), is the interconnection protocol of choice between communication providers and their customers. SIP signalling establishes a session between one or more end points which in the telephony sector are usually audio in nature but can also support video and message based communications (Internet Engineering Task Force, 2002). A SIP device can be a handset (Cisco, Yealink, Avaya to name a few) or a routing device such as a PBX or Session Border Controller.

It is common for one SIP device to probe another SIP device to understand its parameters and features. This is known as an Option (Internet Engineering Task Force, 2002). Once a device understands the third-party device (such as that between a handset and a PBX), a Registration can take place. This is similar to authentication of an email server. Therefore, when a phone call is made, the device making the call will send an Invite to the intended third party with details of the proposed communication. If the proposed communication is acceptable, a session can be established (Internet Engineering Task Force, 2002). It is important to note that a Registration is not required for an Invite to be sent, in this scenario it is common in the SIP Trunking world (i.e between PBX and Supplier) where two parties trust each others IP which is known as IP Authentication[5].

PBX design and features have grown considerably in recent years and enable a wide range of features such as conference rooms, remote working for staff and its not uncommon for large global organisations to run their entire communication systems on their PBX to enable Unified Communications. Some PBX's are now focusing on providing this functionality[6].

2.2 PBX Penetration Studies

Sengar suggests poor configuration and lack of complex credentials rather than SIP vulnerabilities are the reasons why SIP systems are compromised (Sengar, 2014).

In 2012 the findings of a 2-year distributed Honeypot (Honeynet) experiment by researchers from the University of Essen, Germany witnessed over 47.5 million SIP messages. They further went on to describe behaviour that was noticed in the form of 4 stages to an attack. The authors noted that some parts of an attack were automated, while others were not (Hoffstadt et al., 2012). During this period, other researchers such as those from the Vienna University of Technology were also running a SIP Honeynet (Gruber et al., 2013). There findings were similar in that hackers attempted to call African countries such as Ethiopia and Egypt and calls originated from an Egyptian IP (Hoffstadt et al., 2012), (Gruber et al., 2013).

Shortly prior to this research, the researchers of this paper conducted a 10-day Honeypot experiment that focused whether attacker methodology had changed. Unlike the Essen and Vienna experiment, the researchers at the University of Southampton used a real, well known PBX (FreePBX[7]). The researchers only focused on opening and studying SIP Ports. The findings in this short period of time were considerable in comparison to previous research. In 10 days, the Honeypot received approximately 19 million SIP Messages with most Invites originating from France and the United States. The experiment also suffered a significant attack during 1 day which resulted in system resources mostly being consumed during the period that had similar characteristics of Distributed Denial of Service attack (McInnes et al., 2019).

2.3 Consequences of Attacks

The consequences of an attack are rarely reported but can be catastrophic for small organisations. The cost of attacks can be extremely high, and costs can rise to business fatal amounts within a very short period of time. In 2014 a business was reported to receive a

[5] https://support.voicepulse.com/hc/en-us/articles/202526945-What-is-IP-Authentication-

[6] https://www.3cx.com/pbx/unified-communications/

[7] https://www.freepbx.org

bill from their communications provider of $166,000 after their PBX was hacked over a weekend period (New York Times, 2014). In similar situations, litigation cases were brought in the UK (£30,000+ Phone Bill) (His Honour Judge David Grant (Bailii.org), 2014) and Netherlands (€176,000+ Phone Bill) (Central Netherlands District Court, 2014).

Furthermore, the FBI noted a case where the group behind the Mumbai 2008 bombings had received funding by PBX Hacking (not specifically for an individual attack) (Lisa Vaas, 2011). This general thought of terrorist groups being funded by PBX Hacking and general telecommunication fraud is further reinforced by a former corporate security fraud manager at a large global telecommunications operator[8].

Europol in a joint report with TrendMicro claim that telephony fraud is originating in failed states and *"being used to prop up failing economies"* (Europol and Trend Micro, 2019).

2.4 Advance Persistent Threat (Kill Chain)

The Cyber Kill Chain is an adaption of the military use of the term "Kill Chain" by Lockheed Martin to describe how an enemy carries out an attack in cyber space (Lance Spitzner, 2019). Researchers from Lockheed Martin define an Advance Persistent Threat (APT) as actors who are well trained and resourced in performing continual campaigns against their targets in an attempt to acquire information of a confidential nature such as proprietary or national security (Eric M Hutchins and Michael Cloppert and Rohan M Amin, 2011). Tankard describes "Advance" as the skill set of the hackers, along with techniques and exploits used, while "Persistent" refers to their continual attempts in gaining and maintaining access and "Threat" being hard to defend against due to the sophistication (Tankard, 2011). Tankard quotes McAfee as implying the sophistication of techniques used by attackers are only seen the defence sector (Tankard, 2011).

Hutchins et al. define the kill chain as *"a systematic process to target and engage an adversary to create desired effects"* (Eric M Hutchins and Michael Cloppert and Rohan M Amin, 2011). This is true within the context of the Air Force where the kill chain is defined as Find, Fix, Track, Target, Engage, Asses (F2T2EA) (John A Tirpak, 2000). Hutchins et al. further describes that the cyber equivalent of the kill chain as Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control, Actions on Objectives (Eric M Hutchins and Michael Cloppert and Rohan M Amin, 2011).

3 METHODOLOGY

The Honeypot ran over a 115-day period between 18th October 2018 00:00 BST – 9th February 2019 23:59 GMT. However, due to recording errors (such as the Virtual Machine (VM) becoming full), 12 days were not included in the data sets. Therefore, for the purpose of analysing data, this Honeypot ran for 103-days. Furthermore, for a short period (21 days) between the 20th December 2019 00:00 GMT to 9th January 2020 23:59 GMT the Honeypot experiment was setup in a basic VoIP Ports monitor only scenario to monitor SIP attacks on the system over the 2019/2020 Christmas period. In this experiment an Invite, Registration and Option have the meaning set out within IETF RFC 3261 (Internet Engineering Task Force, 2002). The main Honeypot was not advertised, except from several weeks earlier when it was used to conduct a 10-day experiment (McInnes et al., 2019).

Unlike historic research from over 6 years ago (Essen and Vienna), this Honeypot used a well-known and distributed PBX called FreePBX[9]. The benefit of this is that meta data exchanged in Invites, Registrations and Options would provide details on the PBX such as software version.

3.1 PBX Configuration

The Honeypot was set up in a similar configuration to the 10-day Honeypot that was previously conducted (McInnes et al., 2019). The location of the VM was London, United Kingdom.

In addition to the SIP ports (TCP/UDP 5060 – 5070) being opened as per the 10-day experiment (McInnes et al., 2019), ports 80 and 443 were also opened to monitor any web traffic attempts. To prevent any attacker successfully gaining access, the .htaccess was modified to allow access from specific IPs, but ultimately would log if any connection attempt had been made. The same SIP user accounts that were created in the 10-day experiment were also used in this experiment in an attempt to see if hackers are able to successfully authenticate through brute force.

There were various options to capturing data, such as Packet Analysis, Asterisk Log and Apache Logs.

[8] https://riskandassurancegroup.org/telecoms-fraud-terrorism-and-money-laundering-by-david-morrow-of-fraud-fit/

[9] https://www.freepbx.org

A similar method used in the 10-day experiment (McInnes et al., 2019) was also used in this experiment. To investigate and note any trends, Wireshark was used to extract knowledge out of the results using the tools built in to summarise key information on both SIP and Web protocols. To make sure results were not skewed by our own activity, we have made sure that our access has been omitted from the results.

3.2 PBX Security

The security of the experiment is important as the objective is to observe hack attempts, but not actually get hacked itself. Therefore, several techniques were used to enable this.

The VM provider provided a firewall at the cloud level. Therefore, by default all ports were closed except SIP and Web Ports. The SSH port for controlling the server was opened up to only allow connections from a select number of IPs. In addition to this, to prevent third parties from the VM provider seeing any of the data, disk encryption was also used on the VM partition using LUKS at the OS Level. Furthermore, as discussed in the previous section, a .htaccess file was used to control the files any potential hacker could access if they attempted to access via the web ports. Finally, the PBX came with a feature called Fail2Ban that could ban IP addresses on certain parameters being met. Although in the real world this may help, in our experiment this feature could impede us collecting full results to demonstrate the scale of such problem. Therefore, this feature was disabled.

4 RESULTS

During the 103-day period, the Honeypot encountered 100,898,222 inward SIP messages. This is a mean average of 979,594 messages per day. A sample of these days can be seen in Table 1. During the experiment only 0.03% of all Registration attempts registered successfully. During the 103-day period all extensions that had the same username and password combination registered successfully. During this experiment, the system resources were not actively monitored although on occasions the CPU was 80% when attackers conducted attacks in short time periods.

Table 1: Summary Breakdown of SIP Messages Received.

	SIP Message Type Received		
Date	**Register**	**Invite**	**Option**
18/10/2018	265,365	155	64
19/10/2018	243,161	23,621	78
. . . .			
08/02/2019	133,245	12,081	2,779
09/02/2019	555,654	5,867	1,240
Total	98,928,641	1,790,648	179,633

4.1 Attack Origination

During the 103-day Honeypot period, the Honeypot received SIP messages originating from 732 different IP subnets from 45 different countries. Table 2 demonstrates the most popular IP Subnets. In this experiment an IP Subnet means a /24 IP range where the last octet has been removed for data privacy reasons.

Table 2: Top Countries of IP /24 subnets Observed.

Country	**Amount**
France	199
United States	186
Palestine Territories	70
Germany	45
Netherlands	40
Canada	30
Russia	29
United Kingdom	16
Poland	14
Italy	11
Other	92
Total	732

4.2 Christmas 2018 Slow Down

During the 2018 Christmas period, there was a significant slowdown in attacks of Registrations, Invites and Options. Specifically, on Boxing Day 2018, the Registrations were the lowest by a significant margin recorded during the entire 103-day Honeypot period. The lowest Registration and Invites were witnessed during this period and have been underlined in Table 3. The SIP messages daily mean average during the Christmas 2018 period (excluding 24/12/2018 as there is a large difference) is 153,575.

During the Christmas period of 2019, the Honeypot ran for a short period between the 20th December 2019 to 9th January 2020. During this period there was no slow down over the Christmas period. Only the basic Registration, Invites and Options were observed. There was a total of 11,919,525 SIP Messages received during the 21 days. Table 4 contains

Table 3: Christmas 2018 SIP Messages Received.

	SIP Message Type Received		
Date	**Register**	**Invite**	**Option**
24/12/2018	4,420,467	5,397	326
25/12/2018	2,409	3,828	326
26/12/2018	404	887	758
27/12/2018	83,294	935	101
28/12/2018	94,588	738	881
29/12/2018	109,225	1,596	403
30/12/2018	312,117	1,596	804
31/12/2018	460,416	145	133

the Christmas 2019 break down comparison to the same period in 2018. The SIP messages daily mean average during the 2019 Christmas period (excluding 24/12/2019 to compare the same date range) is 746,222 (567,596 messages per day if considering the 21 day period the Honeypot ran for.)

Table 4: Christmas 2019 SIP Messages Received.

	SIP Message Type Received		
Date	**Register**	**Invite**	**Option**
24/12/2018	422,690	12,251	1,024
25/12/2018	377,845	15,684	289
26/12/2018	207,709	10,725	740
27/12/2018	775,099	7,142	747
28/12/2018	608,075	10,323	896
29/12/2018	1,742,582	7,284	172
30/12/2018	340,244	14,421	4,114
31/12/2018	1,089,406	8,449	1,605

4.3 Unauthenticated Invites

During the 103-day experiment, there were 1,170,828 call attempts across 1720 telephone numbers in 119 countries (including numbers that were internal extensions and numbers not known). The most popular countries along with their proportion of numbers can be seen in Table 5.

To summarise there were 1,790,648 Invites, but overall there were 1,170,828 call attempts. This is because when an attacker attempts a call, it may get rejected, therefore they may try to authenticate and then send the Invite again. This would be classed as 1 call attempt. The majority of these numbers were low cost and not premium in nature.

Figure 1 shows the disruption of IP subnets that generated the call attempts.

In this experiment the following countries were observed with having 6 or more digits in their prefix when attempting to call out:

Table 5: Individual Numbers Observed.

Country	Unique Numbers	Total Call Attempts	Percent of Invites
United States	522	127,077	10.9%
Unknown	189	1,218	0.1%
United Kingdom	126	453,791	38.8%
Germany	122	142,911	12.2%
Israel	80	44,841	3.8%
Poland	52	147,765	12.6%
Turkey	46	65	0.0%
Sri Lanka	34	34	0.0%
Myanmar	33	34	0.0%
Norway	28	136,621	11.7%
Other	448	116,471	9.9%

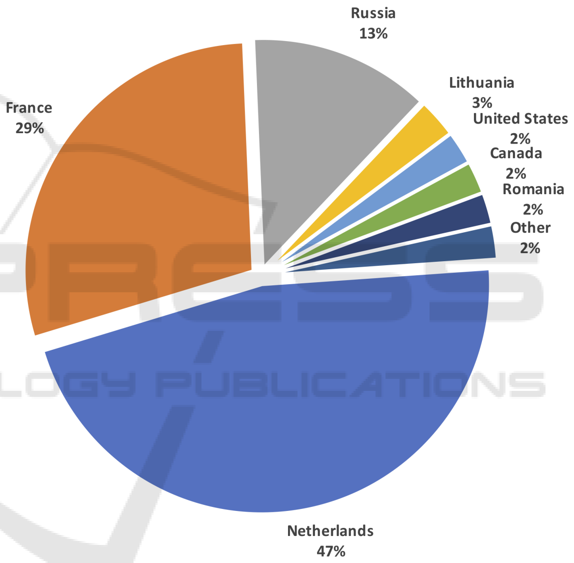


Figure 1: Top Countries where Invites Originated from based on IP /24 Subnet.

- Argentina
- Belgium
- France
- Germany
- Ireland
- Israel
- Netherlands
- Norway
- Palestinian Terr.
- Poland
- Spain
- Sweden
- United Kingdom

4.4 SQL Injection Invites

During the detailed analysis of Invites, peculiar activity was observed in some of the *"From"* head-

Table 6: Sample SQL Injection SIP Headers.

From	**To**
or”=’⟨sip:’or”=’@IP⟩	97059995XXXX ⟨sip:97059995XXXX@IP⟩
⟨sip:’or”=’@IP⟩	⟨sip:90114681240XXXX@IP⟩
4+2=11⟨sip:4+2=11@IP⟩	0221518595XXXX⟨sip:0221518595XXXX@IP⟩
a’or’3=3–⟨sip:a’or’3=3–@IP⟩	003375677XXXX⟨sip:003375677XXXX@IP⟩
⟨sip:&=_72ZyTaKvw5CvD4urd@IP⟩	⟨sip:0044190491XXXX@IP⟩

Table 7: Common SQL related resources being attempted.

URL	**Count of Resource attempted**
/phpMyAdmin/scripts/setup.php	189
/phpmyadmin/scripts/db___.init.php	83
/mysql/sqlmanager/index.php	25
/phpMyAdmin/	19
/DownFile.php?filename=../../../../../../../../etc/passwd%00	2
/estadisticas/download.php?csv=../../../../../../../../../etc/passwd	2
/download_file.php?file=../../../../../etc/passwd	2
/export.php?export=../../../../../../../../../etc/passwd	2

ers within the Invite messages being received by the Honeypot PBX. These “From” headers were receiving non-numerical characters. On detailed inspection, it was realised that these were SQL injection attempts. Some examples can be seen in Table 6.

4.5 URL Accessed

During the 103-day period, web ports were observed in an attempt to see what, if any activity, occurred on web ports and do attackers attempt to gain access or an advantage using web ports? There was a total of 43,872 resource requests made, to a total of 1856 different URLs on port 80. On port 443 (Secure Socket Layer), there were 15,680 resources requested where 1,222 were unique.

During the 103-day period, there was a significant continual attempt to access SQL database management software known as PhPMyAdmin[10]. Additionally, there were regular attempts to access the /etc/passwd file on the Linux Server through path traversal attacks[11]. It was observed where a VoIP based resource was attempted to be accessed on port 80, it would regularly follow the redirection to port 443. However, most non-VoIP based resources did not follow, or attempt on port 443. Examples of these can be seen in Table 7.

Many of the attempted URLs were not thought to be VoIP or PBX related. Therefore, these were called noise. Most SQL and traversal were noise, although as discussed later some were also VoIP Based. Table 8 contains the top 10 accessed VoIP Resources on Port 80.

The most attempted page accessed is the PBX admin configuration page (/admin/config.php). The second most popular is the recordings folder. The third most accessed resource was the administrative interface for an open source VoIP Billing software (A2billing[12]). The different URL’s witnessed in relation to A2billing, attempted to make use of a security vulnerability which allowed database backups[13]. By gaining access to this, attackers would have the raw SIP credentials to be able to facilitate their attacks (among other customer data resulting in a significant data breach). These can be seen in Table 9.

It was also observed that a traversal attack was attempted using a vulnerability in the vtigerCRM software in an attempt to access the Asterisk sip.conf [14] file which could facilitate access to SIP credentials that may exist[15]. Vtiger is a Customer Relationship Manager (CRM) software which contains a telephony gateway[16]. These specific attempts can be seen in more detail in Table 9.

When analysing the URLs that were attempted, it was noticed that names of devices were regularly appearing. On further investigation, these are provisioning folders or files potentially containing cre-

[10] https://www.phpmyadmin.net

[11] https://owasp.org/www-community/attacks/Path_Traversal

[12] http://www.asterisk2billing.org

[13] https://www.exploit-db.com/exploits/42616

[14] http://www.asteriskdocs.org/en/3rd_Edition/asterisk-book-html-chunk/DeviceConfig_id216341.html

[15] https://www.exploit-db.com/exploits/35574

[16] https://www.vtiger.com/docs/phone-calls

Table 8: Top 10 VoIP Resources requested.

URL	Count of URL
/admin/config.php	23,857
/recordings/	325
/a2billing/admin/Public/index.php	311
/recordings/page.framework.php	69
/vtigercrm/vtigerservice.php	32
//recordings/	25
/recordings/index.php	19
/_asterisk/	19
/vtigercrm/modules/com_vtiger_workflow/sortfieldsjson.php?module_name=..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fetc %2fasterisk%2fsip.conf%00	17
/digium_phones/	16

Table 9: A2billing and VTiger Vulnerability Examples.

URL	Count of URL
/a2billing/admin/Public/A2B_entity_backup.php?form_action=add&path=/var/www/html/_asterisk/.txt	2
/a2billing/admin/Public/A2B_entity_backup.php?form_action=add&path=/var/www/html/assets/.txt	2
/a2billing/admin/Public/A2B_entity_backup.php?form_action=add&path=/var/www/html/recordings/.txt	2
/a2billing/admin/Public/A2B_entity_backup.php?form_action=add&path=/var/www/html/var/.txt	2
/vtigercrm/graph.php?module=../../../../../../../..//etc/passwd%00	1
/vtigercrm/graph.php?module=/etc/passwd%00	1
/vtigercrm/modules/backup/page.backup.php?action=download&dir=/etc/passwd	1

dential details for a specific phone. This could infer there is a vulnerability in this method of provisioning phones. In addition, Table 8 contains the folder "/digium_phones/" which is used by handsets for configuration and provisioning[17].

The IP Subnet data collected on URLs were cross referenced with that witnessed in SIP Attacks. On port 80, there were 2,618 different IP subnets observed. When cross referencing these, 68 subnets were found to be in common. It was observed that a Dutch IP subnet that resulted in the highest amount of data for any individual subnet on SIP attacks was also the subnet that was responsible for the largest amount of VoIP Based URL attempts and was responsible for a large portion of URL attempts to the admin configuration panel, along with attempts to exploit A2billing vulnerabilities and the recordings folder.

5 DISCUSSION OF RESULTS

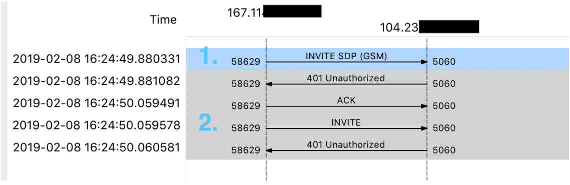
The 103-day experiment has re-enforced the original findings of the original 10-day experiment (McInnes et al., 2019), but with providing an improved estimate of the scale due to its prolonged duration. If this experiment were to run for the same duration as that of the Essen Honeynet (771 days) (Hoffstadt et al., 2012) then it is projected there would be 760 million SIP messages which is more than 16 times the scale. This is more accurate than the 30 times the scale finding due to 1 day skewing the results because of a large attack in the 10-day experiment (McInnes et al., 2019). Furthermore, it is worth considering that this is just 1 Honeypot, where the Essen experiment had several Honeypots to make up a Honeynet. Either way, this demonstrates the size of attacks have increased significantly since the Essen Honeynet began.

It was observed through Wireshark, there were a large number of Invites compared to total call attempts. This can be explained either because the PBX was overloaded and had not responded fast enough and therefore resent or (most occasions) was because

[17] https://support.digium.com/s/article/Why-can-t-I-update-phone-firmware-or-custom-ringtones-after-a-FreePBX-update

the PBX would send a 401 requesting the attacker to Register (i.e. their Invite was unauthenticated), at which point the attacker would send the same Invite again, but with registration details. This signalling flow can be observed in Figure 2.

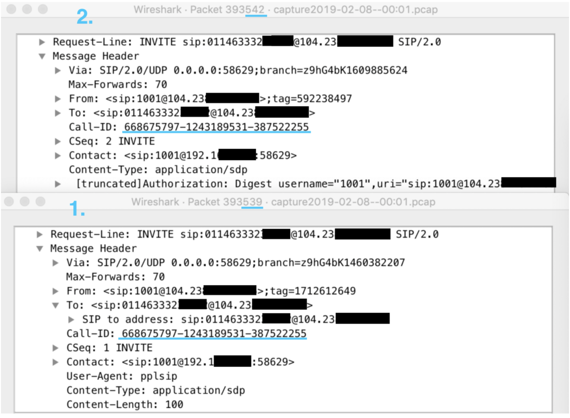
The difference in call attempts can be seen in the SIP Invite messages (Figure 3) where the Call-ID are the same, meaning the same call attempt, but the caller attempts to authenticate. This is an alternative way of Registering with a PBX than directly Registering.



```
Time                             167.11[redacted]
                                                     104.23[redacted]
2019-02-08 16:24:49.880331  1.  58629  INVITE SDP (GSM)  →  5060
2019-02-08 16:24:49.881082      58629  ←  401 Unauthorized  5060
2019-02-08 16:24:50.059491      58629  ACK  →               5060
2019-02-08 16:24:50.059578  2.  58629  INVITE  →            5060
2019-02-08 16:24:50.060581      58629  ←  401 Unauthorized  5060
```

Figure 2: Wireshark Unauthorised Invite Attempt.

On detailed inspection, it can be seen the attacker is attempting to make the IP source (from header) of the call appear as if it is coming from the PBX itself suggesting that there is a vulnerability that some systems would allow the call to go through as the PBX may be tricked into believing the call originated internally. 104.23….. is the IP of the PBX Honeypot and it can be observed that the number beginning 011463332 is a Swedish number where 011 is the prefix being used to dial international from a North American country. This could suggest that some telephony systems are vulnerable to this method of attack (i.e. if the IP is local to the machine, then skip authentication).



2\.

Wireshark · Packet 393542 · capture2019-02-08--00:01.pcap

```
▶ Request-Line: INVITE sip:011463332[redacted]@104.23[redacted] SIP/2.0
▼ Message Header
  ▶ Via: SIP/2.0/UDP 0.0.0.0:58629;branch=z9hG4bK1609885624
    Max-Forwards: 70
  ▶ From: <sip:1001@104.23[redacted]>;tag=592238497
  ▶ To: <sip:011463332[redacted]@104.23[redacted]>
    Call-ID: 668675797-1243189531-387522255
  ▶ CSeq: 2 INVITE
  ▶ Contact: <sip:1001@192.1[redacted]:58629>
    Content-Type: application/sdp
  ▶  [truncated]Authorization: Digest username="1001",uri="sip:1001@104.23[redacted]
```

1\.

Wireshark · Packet 393539 · capture2019-02-08--00:01.pcap

```
▶ Request-Line: INVITE sip:011463332[redacted]@104.23[redacted] SIP/2.0
▼ Message Header
  ▶ Via: SIP/2.0/UDP 0.0.0.0:58629;branch=z9hG4bK1460382207
    Max-Forwards: 70
  ▶ From: <sip:1001@104.23[redacted]>;tag=1712612649
  ▼ To: <sip:011463332[redacted]@104.23[redacted]>
    ▶ SIP to address: sip:011463332[redacted]@104.23[redacted]
    Call-ID: 668675797-1243189531-387522255
  ▶ CSeq: 1 INVITE
  ▶ Contact: <sip:1001@192.1[redacted]:58629>
    User-Agent: pplsip
    Content-Type: application/sdp
    Content-Length: 100
```

Figure 3: Wireshark Authenticated Invite Attempts.

The same user agents that were detected in the 10-day Honeypot (McInnes et al., 2019) were also detected in this experiment. As seen in Figure 3, "pplsip" is the user agent used in this Invite. However, on other occasions as similar to the 10-day Honeypot, user agents were giving the impression of other VoIP Equipment being used to attack the PBX Honeypot (Such as Avaya, Cisco etc.).

In the 10-day experiment (McInnes et al., 2019), it was suggested that SIP hardware has been compromised (due to various user agents appearing to be hardware). It could also suggest attackers are attempting to trick the PBX into believing that specific equipment is attempting to make use of the PBX as a method of overcoming authentication requirements or hiding attack attempts. This can further be expanded to suggest another theory and reinforce a botnet idea that there is a botnet of different hacked devices. As witnessed in the web traversal attempts, access to the /etc/passwd file on Linux system would provide the ability for the attacker to compromise and control that system, adding it to a botnet. This may explain how so many systems appear to be involved attacking.

Essen researchers concluded that different attackers were involved in different elements of the attack (Hoffstadt et al., 2012). Based on this Honeypot, it would reinforce the 10-day Honeypot suggestion that there is now a botnet involved in attempting to hack PBXs due to the distribution of IPs witnessed and the wide variety of equipment that is claimed to be used.

The Essen researchers made a claim that attackers shared data between themselves (Hoffstadt et al., 2012). This does remain valid, but this may have been mistaken for botnet activity which is better understood today as the actual attackers appear to be the same (Christmas slow down – discussed later on), but their means are to use systems that are distributed to attack the Honeypot making it harder to block if a system needs to remain open as users are geographically distributed (i.e. not on the same network).

There were only IP Subnets in 45 countries over 103 days witnessed, which is significantly less than the 75+ countries witnessed in the 10-day Honeypot. This could be because the machines available to attackers are always changing.

When analysing IP Subnets, it was observed that Invite IPs were rarely the same as registration IP Subnets. Although there is a large number of examples where attackers already knew the extension numbers of extensions when sending Invites. This may be because a similar configuration was used previously, and the attackers have this information stored (10-day experiment (McInnes et al., 2019)). This can also be determined through trying to Register as different error codes are sent by the PBX when the credentials are wrong, or a user does not exist. Therefore, over time an attacker could build a list of users. It was also observed that over 50% of Invites had they're *"From"* header set as a valid extension number, although there had been no Registration from those IPs. This can be seen in Figure 3. It is not always a requirement to authenticate with a username/password. Calls can be authenticated through Caller Line Identity (CLI) which may explain why attackers attempted to use known extensions. Furthermore, some systems may also be vulnerable to SQL Injections after similarly seeing attempts in the *"from"* SIP signalling header as shown in Table 6. This could be attempting to bypass authentication through SQL injection where calling is based on CLI Authentication which would reinforce that some systems could be vulnerable and do there authentication based on extensions as witnessed earlier where many Invites contained valid extension numbers.

The level of the sophisticated nature and persistence of these attacks demonstrates similarities to that of the background literature discussed Kill Chain and an Advance Persistent Threat (APT). This is demonstrated by the witnessed qualities:

- Advance:
  - Attackers use a large range of methodologies and vulnerabilities in software and misconfigurations across various web and VoIP attack vectors.
  - Utilising complexity of cross border stakeholders involved in the Call Chain.
  - Attackers appear to originate from many countries.
  - Attackers have over 1,000 low-cost numbers available to them (logistically complicated to manage this setup) suggesting stealthy based behaviour in an attempt to be able to call out without raising suspicion prior to main attack. This is similar to behaviour identified historically by C. Yates[18], although many of the numbers witnessed in our experiment would be classed as regular landline numbers.
- Persistent:
  - On connection to the internet, PBX system is under attack soon after. Almost appearing every minute of every day.
  - Previous research suggests once attackers gain access they do not call immediately, although our research showed attackers were attempting numbers persistently.
- Threat:
  - Spectrum of vectors used by attackers means only way to defend is to block all ports on a firewall, but this action would significantly limit functionality.

In addition, the sophistication, automation and resources (numbering, suspected botnets etc.) available to the attackers demonstrated by monitoring web ports showed the lengths attackers would go to in an attempt to get access to SIP credentials and make calls. Cross referencing of IPs demonstrated that the same attackers are involved in multi-vector type attacks to gain access. Furthermore, the large amount of money involved would require specialist skills to launder the significant scale of money involved in these frauds (possibly across multiple borders, outside the telephony network). It would be difficult to believe if this was a lone actor conducting these attacks, but a sponsored group who are well organised. Given the geographical spread of IP's involved it is difficult to determine where these attackers are actually located. However, during Christmas 2018 (Table 3) the attacks significantly decreased, which defies logic considering phones systems would most likely have less attention given to them during this time period and attacks could be more profitable if an attack is successful. This provides the impression that attackers possibly celebrate Christmas and the operation still has significant human oversight. It also suggests given the large reduction in attack frequency, it was possible only 1 or a small handful of attackers were involved in attacking our Honeypot. During Christmas 2019 (Table 4), the Honeypot was repeated and during this time, there was no slow down. This could be explained by an apparent improvement in automation of the operation since the original Hoffstadt et al. experiment.

This sophistication is evident in the web protocol monitoring which saw vulnerabilities in PBXs and VoIP software attempting to be exploited. If these vulnerabilities were exploited it could have not only provided the attacker with SIP credentials, but also personal data (CRM and billing systems) which could provide extra value to attackers if they were to sell this data on.

Expanding previous research investigating PBX hacking as a whole, this research has demonstrated that PBX hacking has become highly sophisticated when compared to previous studies. The multi-vector (SIP and Web) based methods would require a lot of resources and planning. Due to the large number of attacks, the methodologies involved and sophisticated nature with some IP subnets being involved in cross vector attacks, it is unlikely to be a large number of entities involved. This is based on the following evidence:

[18] http://www.yatesfraudconsulting.com/prism-irsf-db/

- Over 1000 numbers setup in over 100 countries.
- Attacks originate between 700-800 IP Subnets.
- Highly specialised and niche fraud where significant understanding of the sector is required.
- With the value of money being moved, specialised cross border money laundering skills are required.

In comparison to the Essen Honeynet (Hoffstadt et al., 2012) and the 10-day Honeypot (McInnes et al., 2019), this 103-day Honeypot and the additional Christmas 2019 period demonstrates the wide variety of methods attackers are using in an attempt to be able to make outbound phone calls. Furthermore, given the scale of events (SIP and Web based) that have been logged, it would suggest that attackers have improved the automation of their operations. Elements may still be manual, however based on the evidence so far, the money involved and size of the operation, it would suggest this is mostly if not all automated now.

Sengar suggested that poor configuration and lack of complex credentials rather than SIP vulnerabilities are the reasons why SIP systems are compromised (Sengar, 2014). This research has partially confirmed this conjecture through seeing poor SIP credentials as a mechanism for registering with a PBX, although this research has also demonstrated that there is a strong indication that given the methodologies used by the attackers, some methods used are vulnerabilities rather than poor configuration. For example SQL Injection would be a vulnerability at the SIP and database level due to non-escaping rather than controlled within the administrators domain. This is further demonstrated by web based vulnerabilities being used by attackers against configuration web panels. This demonstrates how attackers have become more thorough in there persistence in attempting to infiltrate a VoIP System.

The large number of IP Subnets involved demonstrate the challenges Cloud VoIP and PBX administrators have in attempting to protect against attack, while also not limiting the flexibility, functionality and benefits of NGNs. Due to the high volume of countries where attacks appear to originate, blocking countries may not work. Additionally, attacks appear to originate from well developed countries, so blocking specific countries may not be practical. Given it is also unclear if devices are getting hacked and commandeered into a botnet, a different approach is required around attempting to secure setups. This could include requiring SIP devices to be on the same network through a Virtual Private Network (VPN) connection, implementing features such as Fail2ban (as discussed in the methodology), using provider spend limiting and implementation of other firewall type controls. Although, realistically each setup is different and would need professional consideration around how to secure each setup while maintaining the functionality and benefits PBXs, VoIP and NGN's bring.

6 CONCLUSION

The data and findings of this 103-day Honeypot has demonstrated the increase in threats facing PBX owners. Following on shortly after a 10-day Honeypot (McInnes et al., 2019), this experiment has on balance through a longer run experiment shown that attacks are on average 16 times more aggressive than historic research in this area.

This experiment was configured similar to a previous 10-day Honeypot (McInnes et al., 2019). This Honeypot (unlike the 10-day experiment) also monitored web ports for hacking attempts in addition to VoIP ports. In doing so it witnessed that attackers are multi-discipline in nature by conducting attacks not only on VoIP protocols, but also web protocols, where in some cases these were from the same IP subnets. This research witnessed attempts to make use of vulnerabilities in popular VoIP based software for management and billing used by businesses and providers respectively to either gain access to these systems for gathering SIP credentials or to possibly commandeer to add to a botnet. This experiment also witnessed unlike previous research, SQL injection style attacks in the SIP signalling message suggesting that some SIP systems are vulnerable to malformed SIP headers.

This research saw 100,898,222 SIP messages (excluding Christmas 2019) in 103 days from over 732 IP subnets in 45 countries. Furthermore, it observed 1,170,828 call attempts to 1720 different numbers in 119 countries. It was witnessed that many of these attempts appeared to originate from the Honeypot IP address in the *"From"* SIP header which suggests a poorly implemented authentication vulnerability exists in certain equipment. Furthermore, given the scale of events this research logged, including how Christmas 2018 attacks subsided, while Christmas 2019 continued, it would suggest the attackers operation is now mostly, if not fully automated.

Given the background literature suggesting that telecom fraud is *"being used to prop up failing economies"* (Europol and Trend Micro, 2019), along with the expected revenue this type of fraud generates and the technical complexity, sophistication in multiple disciplines and scale in terms of attack sizes, this research suggests there is an APT dedicated to PBX hacking to conduct Toll Fraud.

Finally, as this research has demonstrated that attacks are growing in sophistication and that attacks are multi-vector in nature, the Honeypot experiment could be repeated, but this time monitoring other protocols to see if attackers who are involved in VoIP Hacking (through VoIP and Web protocols), are also attempting to break into PBXs via other protocols.

ACKNOWLEDGEMENTS

This work was supported by the Digital Economy programme, led by the Engineering and Physical Sciences Research Council on behalf of UK Research and Innovation.

Acknowledgement would also like to be given E.J. Zaluska who was initially involved with the supervision of this research.

REFERENCES

Central Netherlands District Court (2014). Zoekresultaat - inzien document ecli:nl:rbmne:2014:2617. https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBMNE:2014:2617 - Retrieved December 10, 2020.

Colin, D. and Richard, C. T. (2019). *Detecting and Combating Internet Telephony Fraud - Crime Solvability Factors*, pages 127–148. Springer.

Eric M Hutchins and Michael Cloppert and Rohan M Amin (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf - Retrieved December 10, 2020.

Europol and Trend Micro (2018). Toll fraud, international revenue share fraud and more. https://www.europol.europa.eu/sites/default/files/documents/cytel_fraud_intelligence_notification.pdf - Retrieved December 10, 2020.

Europol and Trend Micro (2019). Cyber-telecom crime report 2019. https://www.europol.europa.eu/sites/default/files/documents/cyber-telecom_crime_report_2019_public.pdf - Retrieved December 10, 2020.

Gruber, M., Schanes, C., Fankhauser, F., and Grechenig, T. (2013). Voice calls for free: How the black market establishes free phone calls-trapped and uncovered by a voip honeynet. In *2013 11th Annual Conference on Privacy, Security and Trust, PST 2013*, pages 205–212.

His Honour Judge David Grant (Bailii.org) (2014). Frontier systems ltd trading as voiceflex (claimant) -and- frip finishing ltd (defendant). https://www.bailii.org/ew/cases/EWHC/TCC/2014/1907.html - Retrieved December 10, 2020.

Hoffstadt, D., Marold, A., and Rathgeb, E. P. (2012). Analysis of sip-based threats using a voip honeynet system. In *Proc. of the 11th IEEE Int. Conference on Trust, Security and Privacy in Computing and Communications, TrustCom-2012 - 11th IEEE Int. Conference on Ubiquitous Computing and Communications, IUCC-2012*, pages 541–548.

Internet Engineering Task Force (2002). Sip: Session initiation protocol. https://www.ietf.org/rfc/rfc3261.txt - Retrieved December 10, 2020.

John A Tirpak (2000). Find, fix, track, target, engage, assess. https://www.airforcemag.com/article/0700find/ - Retrieved December 10, 2020.

Lance Spitzner (2019). Applying security awareness to the cyber kill chain. https://www.sans.org/security-awareness-training/blog/applying-security-awareness-cyber-kill-chain - Retrieved December 10, 2020.

Lisa Vaas (2011). Manila at&t hackers tied to terrorist attack in mumbai. https://nakedsecurity.sophos.com/2011/11/30/manila-att-hackers-tied-to-terrorist-attack-in-mumbai/ - Retrieved December 10, 2020.

Marketwired (2016). Argyle data recommendations from cfca's 2015 fraud survey analysis: Think globally, act locally. https://finance.yahoo.com/news/argyle-data-recommendations-cfcas-2015-100000320.html - Retrieved December 10, 2020.

McInnes, N., Wills, G., and Zaluska, E. (2019). Analysis of a pbx toll fraud honeypot. *International Journal for Information Security Research*, 9(1):821–830.

New York Times (2014). Phone hackers dial and redial to steal billions. https://www.nytimes.com/2014/10/20/technology/dial-and-redial-phone-hackers-stealing-billions-.html, Retrieved December 10, 2020.

Ofcom (2007). Regulation of voip services. https://www.ofcom.org.uk/__data/assets/pdf_file/0023/55571/voipstatement.pdf, Retrieved December 10, 2020.

Privsec Report (2017). Telecommunications: the battle against fraud. https://gdpr.report/news/2017/05/29/telecommunications-battle-fraud/ - Retrieved December 10, 2020.

Sengar, H. (2014). Voip fraud: Identifying a wolf in sheep's clothing. In *Proceedings of the ACM Conference on Computer and Communications Security*, pages 334–345.

Tankard, C. (2011). Advanced persistent threats and how to monitor and deter them. *Network Security*, (8):16–19.