NETTITUDE

VOIP Attacks On The Rise

Voice over IP (VoIP) infrastructure has become more susceptible to cyber-attack due to the proliferation of both its use and the tools that can be used for malicious purposes. Nettitude has observed a surge of VoIP attacks against servers around the world over the last few months, but more so in the UK.

This report presents the findings over the first quarter of 2015.

What is VoIP?

VoIP stands for 'Voice over Internet Protocol' and is a way to carry voice and multimedia traffic over computer networks like the internet. Voice signals are converted into digital signals making them easy to transfer over the internet rather than over traditional telephone networks.

There are three main scenarios for VoIP:

1. Computer to computer
2. IP phone to IP phone
3. IP phone/PC to PSTN

The driving factor for the success of VoIP is cost reduction, both for users and providers. But VoIP doesn't only bring reduced costs, it also brings threats and vulnerabilities unprecedented to the telephone industry.

Attacks observed by Nettitude

During the first quarter of 2015, Nettitude observed a large amount of VoIP attacks against the servers we monitor. These often started just a few minutes after a new server went live. Surprisingly, the number of attacks against the VoIP services represented 67% of all attacks recorded against our UK based servers. SQL was the second most attacked service accounting for only 4% of the overall traffic.

This was a different pattern to that seen in other geographies so we decided to take a deeper look into why our UK monitoring systems were being targeted in this way.

The graph in Figure 1 shows the overall services being targeted at for the first quarter of 2015:

Prior to investigating the attacks observed on our servers, let's look at the attack surfaces that VoIP makes available to malicious users.

GENERAL ATTACK STATISTICS

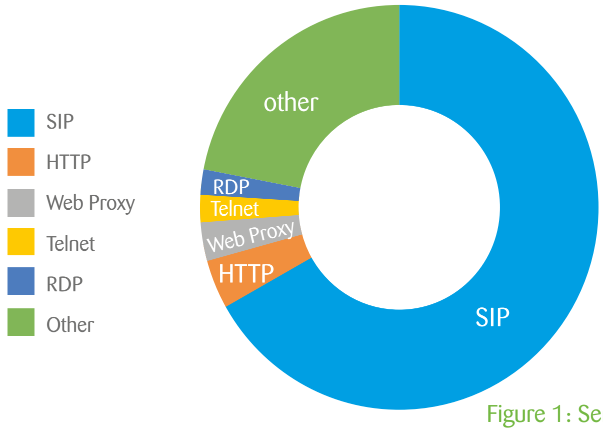


Figure 1: Services targeted Q1 2015

Common threat landscape against Voice over IP infrastructure (VOIP)

VoIP infrastructure is subject to most of the well-known attacks against network infrastructures. However, there are some specific attack vectors that make this a potentially attractive attack surface.

Six categories of threats are recognized by the Voice over IP Security Alliance (VOIPSA) (http://www.voipsa.org/)

1 Social Threats: Social threats can be interpreted as the misrepresentation of identity, authority, rights and content. They also include threats such as the modification of billing records and the generation of unauthorized billing. Unwanted contact is also a consequence of social threats, in instances where an attacker can gain fraudulent access to private company contacts. As a consequence, many users can be contacted without their consent and for malicious purposes. This can lead to harassment and possible extortion. Malicious users can then engage into VoIP spam.

2 Eavesdropping: In this threat category, malicious users are able to monitor VoIP communications between two or more VoIP end points. This can results in call pattern tracking, traffic capture, number harvesting and conversation reconstitution.

3 Interception and Modification: This category refers to threats where a malicious user may have full access to the communication signal between two or more parties. The malicious user can stop the call, change its route and degrade the call, or worse, the attacker can hijack the call and impersonate another legal user.

4 Service Abuse: This category is one of the most common amongst attackers. Premium Rate Service (PRS) fraud is becoming more and more prevalent.

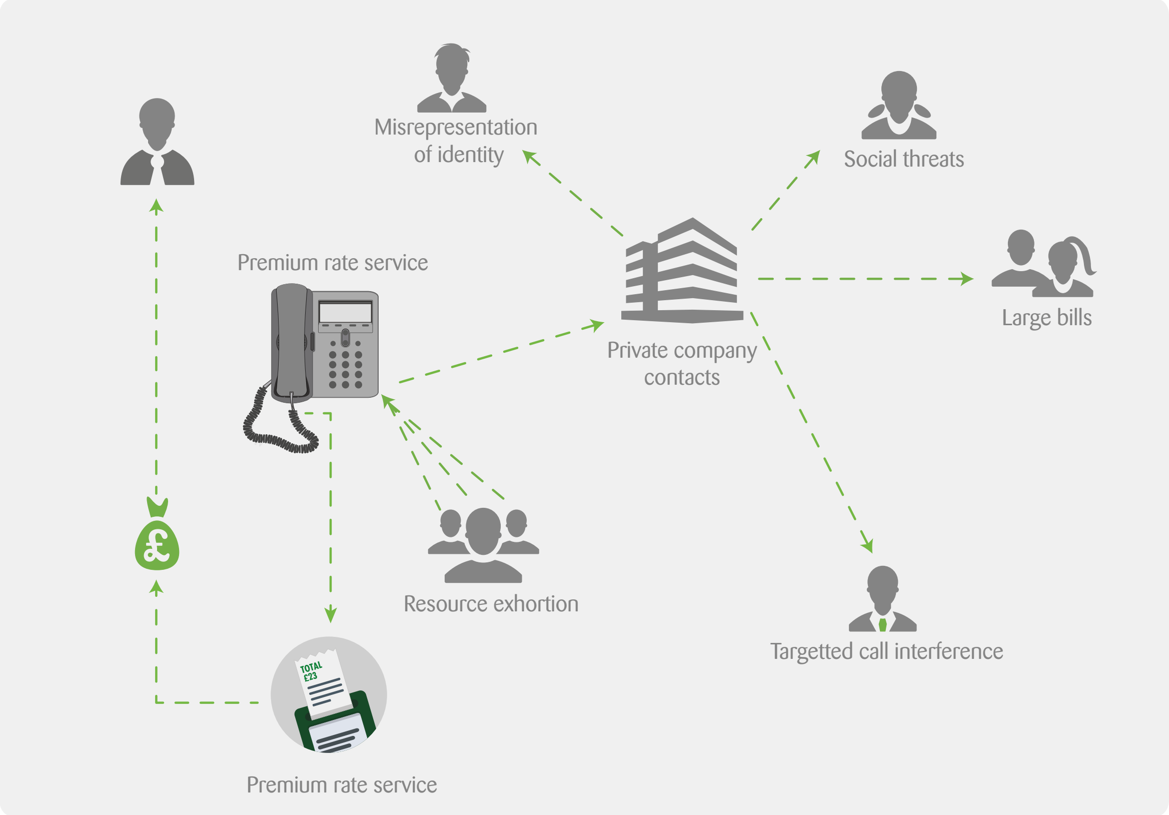


Figure 2: Service abuse illustration

5 Intentional Interruption of Service: VoIP services are subject to denial of service (DoS) attack and resource exhaustion. DoS can be achieved by request flooding, user call flooding, end point request flooding, call controller flooding, request looping, directory flooding, disabling end points with invalid requests, malformed protocol messages, fake call teardown messages, registration hijacking and media session hijacking just to name a few.

It is important to note that an attacker action might have cascading impacts. An attacker may want to test the different options offered by a VoIP server and cause a DoS even though it may not be their main objective. Often DoS situations will mask the real intent.

6 Other Interruptions of Service: This category of threat relates to physical threats such as loss of power.

VoIP Attack Categories

Taking a look at the Open Systems Interconnection (OSI) model, we can soon see that there are various ways in which VoIP traffic and systems can be targeted. A layered approached can be used to categorize VoIP attacks as shown in Figure 3.

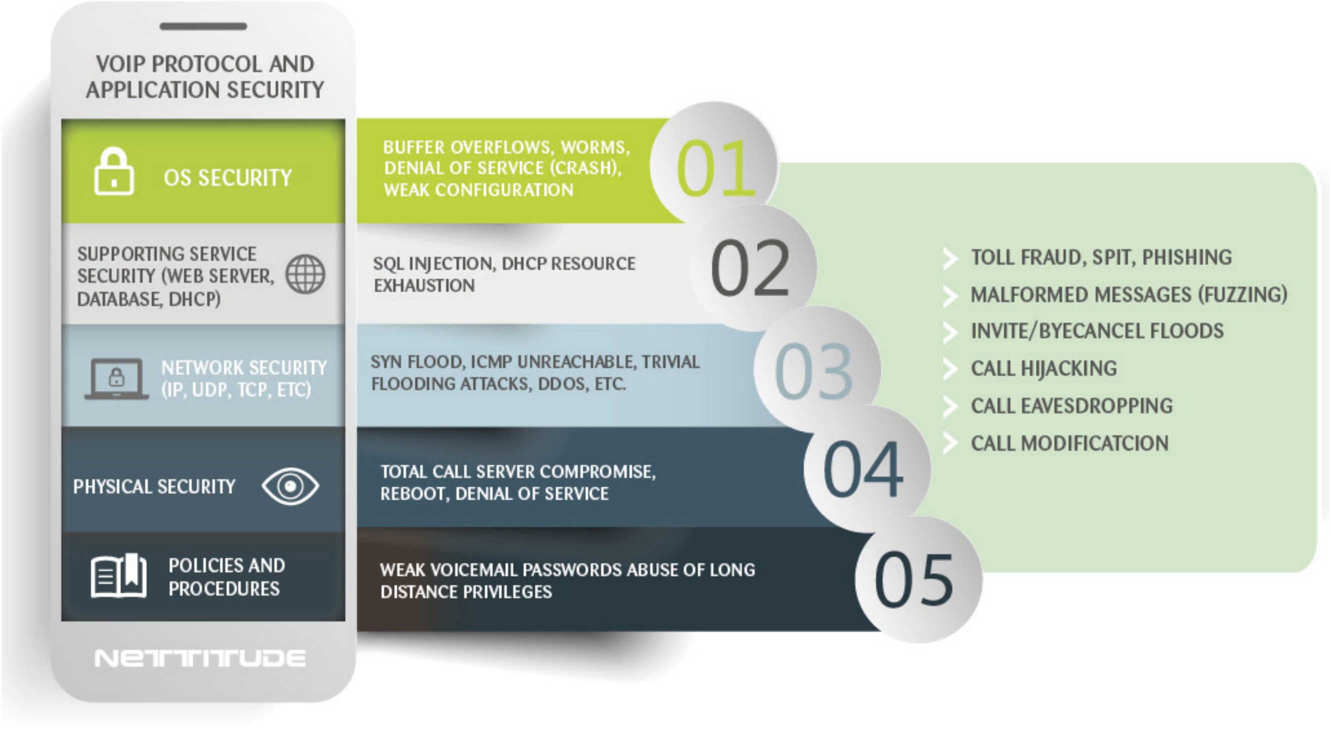
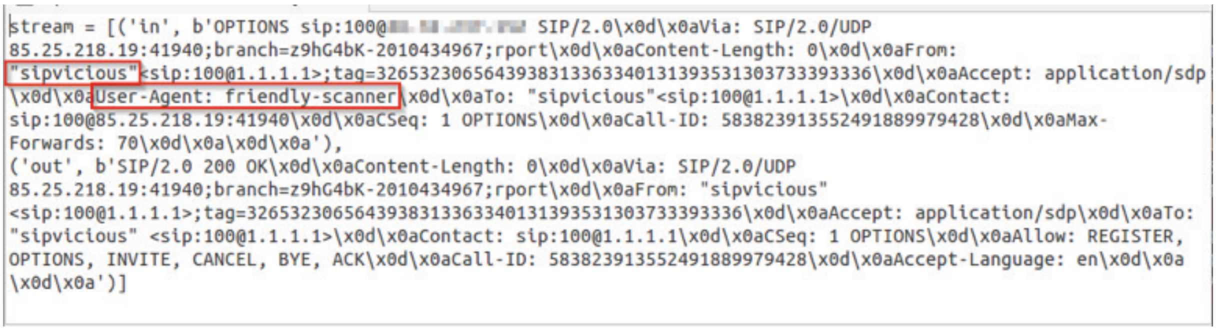

VOIP PROTOCOL AND APPLICATION SECURITY
OS SECURITY
SUPPORTING SERVICE SECURITY (WEB SERVER, DATABASE, DHCP)
NETWORK SECURITY (IP, UDP, TCP, ETC)
PHYSICAL SECURITY
POLICIES AND PROCEDURES
NETTITUDE
BUFFER OVERFLOWS, WORMS, DENIAL OF SERVICE (CRASH), WEAK CONFIGURATION
01
SQL INJECTION, DHCP RESOURCE EXHAUSTION
02
SYN FLOOD, ICMP UNREACHABLE, TRIVIAL FLOODING ATTACKS, DDOS, ETC.
03
TOTAL CALL SERVER COMPROMISE, REBOOT, DENIAL OF SERVICE
04
WEAK VOICEMAIL PASSWORDS ABUSE OF LONG DISTANCE PRIVILEGES
05
TOLL FRAUD, SPIT, PHISHING
MALFORMED MESSAGES (FUZZING)
INVITE/BYECANCEL FLOODS
CALL HIJACKING
CALL EAVESDROPPING
CALL MODIFICATCION

Figure 3: Layered approach to VoIP threat
(Inspired from D. Endler and M. Collier, Hacking Exposed VoIP: Voice Over IP Security Secrets & Solutions 2007)

VoIP attacks, just like any other attacks against network infrastructure, would have different impacts on the business depending on the service that were being targeted.

Tools and techniques used by attackers

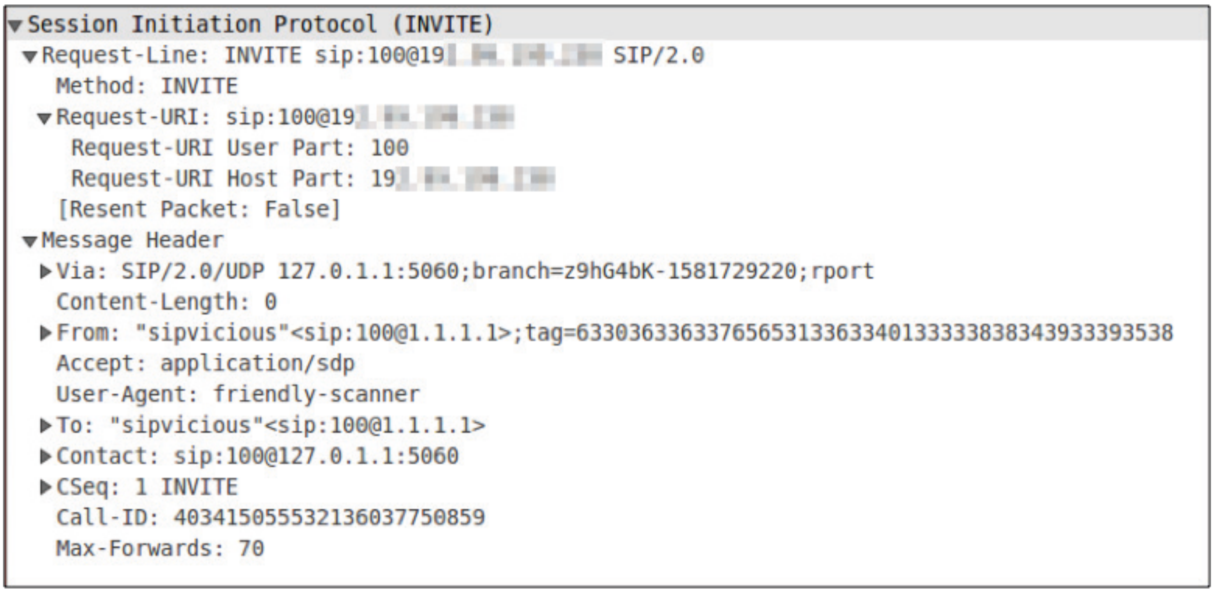
The picture below is a good representation of a short session by a malicious user as captured by our servers. In this session, it is easy to notice that the attacker is using a tool called SIPVicious. We went ahead and downloaded the SIPVicious tool and tested it.



```
stream = [('in', b'OPTIONS sip:100@[redacted] SIP/2.0\x0d\x0aVia: SIP/2.0/UDP
85.25.218.19:41940;branch=z9hG4bK-2010434967;rport\x0d\x0aContent-Length: 0\x0d\x0aFrom:
"sipvicious"<sip:100@1.1.1.1>;tag=3265323065643938313363340131393531303733393336\x0d\x0aAccept: application/sdp
\x0d\x0aUser-Agent: friendly-scanner\x0d\x0aTo: "sipvicious"<sip:100@1.1.1.1>\x0d\x0aContact:
sip:100@85.25.218.19:41940\x0d\x0aCSeq: 1 OPTIONS\x0d\x0aCall-ID: 583823913552491889979428\x0d\x0aMax-
Forwards: 70\x0d\x0a\x0d\x0a'),
('out', b'SIP/2.0 200 OK\x0d\x0aContent-Length: 0\x0d\x0aVia: SIP/2.0/UDP
85.25.218.19:41940;branch=z9hG4bK-2010434967;rport\x0d\x0aFrom: "sipvicious"
<sip:100@1.1.1.1>;tag=3265323065643938313363340131393531303733393336\x0d\x0aAccept: application/sdp\x0d\x0aTo:
"sipvicious" <sip:100@1.1.1.1>\x0d\x0aContact: sip:100@1.1.1.1\x0d\x0aCSeq: 1 OPTIONS\x0d\x0aAllow: REGISTER,
OPTIONS, INVITE, CANCEL, BYE, ACK\x0d\x0aCall-ID: 583823913552491889979428\x0d\x0aAccept-Language: en\x0d\x0a
\x0d\x0a')]
```

Figure 4: Attack trace

Looking at the SIPVicious tool, we can confirm that the attackers used SIPVicious with the default options. The figure below was captured from Wireshark as we tested the SIPVicious tool against one of our servers. The network trace shown in Figure 3 shows that SIPVicious uses friendly-scanner as its user agent.



```
▼Session Initiation Protocol (INVITE)
 ▼Request-Line: INVITE sip:100@19[redacted] SIP/2.0
   Method: INVITE
  ▼Request-URI: sip:100@19[redacted]
    Request-URI User Part: 100
    Request-URI Host Part: 19[redacted]
   [Resent Packet: False]
 ▼Message Header
  ▶Via: SIP/2.0/UDP 127.0.1.1:5060;branch=z9hG4bK-1581729220;rport
   Content-Length: 0
  ▶From: "sipvicious"<sip:100@1.1.1.1>;tag=633036336337656531336334013333383834393393538
   Accept: application/sdp
   User-Agent: friendly-scanner
  ▶To: "sipvicious"<sip:100@1.1.1.1>
  ▶Contact: sip:100@127.0.1.1:5060
  ▶CSeq: 1 INVITE
   Call-ID: 403415055532136037750859
   Max-Forwards: 70
```

Figure 5: SIPVicious network trace

SIPVicious is a set of tools designed to audit SIP systems. However, attackers use the tool to identify potential victims.

SIPVicious offers the following capabilities:

- **svmap** - this is a SIP scanner. It lists SIP devices found on an IP range
- **svwar** - identifies active extensions on a PBX
- **svcrack** - an online password cracker for SIP PBXs
- **svreport** - manages sessions and exports reports in various formats
- **svcrash** - attempts to stop unauthorized svwar and svcrack scans

In essence, using the SIPVicious application, an attacker could potentially determine the type of system behind a VOIP infrastructure and crack any password either online or using a dictionary attack.

Tools	Occurrences	Percentage
friendly-scanner	71524	91.274%
sipcli/v1.8	6677	8.521%
eyeBeam release 1105a stamp 56793	76	0.097%
VaxSIPUserAgent/3.1	42	0.054%
IM-client/OMA1.0 sipML5-v1.2014.03.26	25	0.032%
eyeBeam release 3006o stamp 17551	10	0.013%
Custom SIP Phone	5	0.006%
SipClient 2.99	2	0.003%
cisco	1	0.001%
Total	78362	100.000%

Typically, SIP enabled devices will usually respond on port 5060 and 5061. However, Skinny Client Control Protocol (SCCP) enabled phones (CISCO) will respond on UDP/TCP 2000-2001. Sometimes remote debugging is found on port 17185.

Attackers' activities:

We observed attacks at multiple layers:

- **Policies and procedures:** The attackers employed regular techniques to break into systems protected by weak passwords. We have recorded a large number of failed password attempts.
- **Abuse of long call privileges:** The most popular options when attackers managed to break into the system were to make long distance and premium calls.
- **Network layer:** The large number of failed attempts to log into the system, register and make calls affected the performance of the system. Such behaviour could cause denial of service, making the services unavailable for legitimate users.
- **Application layer:** The application layer was the most affected. Once connected to the SIP server, the attackers queried the SIP options to understand the capabilities of the attacked server. The attackers will then be able to maximise their attacks. We recorded a large number of calls to premium numbers and foreign number. Such actions can have serious financial impacts on the organisation being attacked.

For example, a premium number from BT would cost £1.50 per minute, of which the owner of the premium number will make £1 for each minute of call. Calling premium numbers from abroad will cost even more.

Hypothetically, if an attacker compromised a VoIP server and managed to start calls to rogue services costing £1.50 a minute, the attacker has about 10 hours from which he could generate £9,000 worth of calls. (i.e. 60 min * 10 hours * £1.50 = £9,000).

Further analysis of the attack data received revealed that the attackers, in this case against a UK server, have been very active out of office hours.

Typically, most companies in the UK will operate between 8:AM and 8:PM. We observed 88% of VoIP attacks were realized when there would typically be no security staff to monitor what was happening as shown in Figure 6. This raises the importance of a 24/7 security system.

88% Attacks during downtime

It is a fact that many companies cannot afford security analysts for 24/7 services. The need of dedicated services is then required to ensure that appropriate responses and actions are taken when attacks are identified.

The overall cost of the incident will be a lot more if the price per minute is higher and if multiple sessions are possible at the same time.

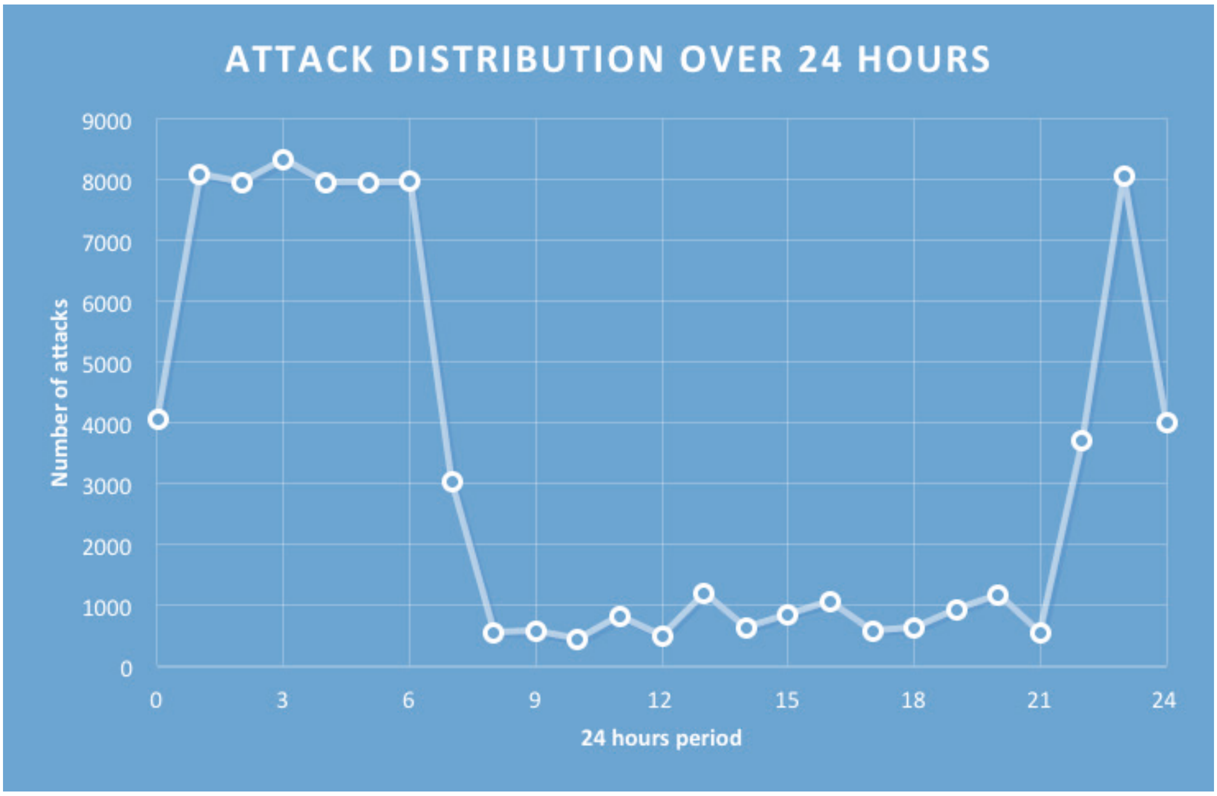
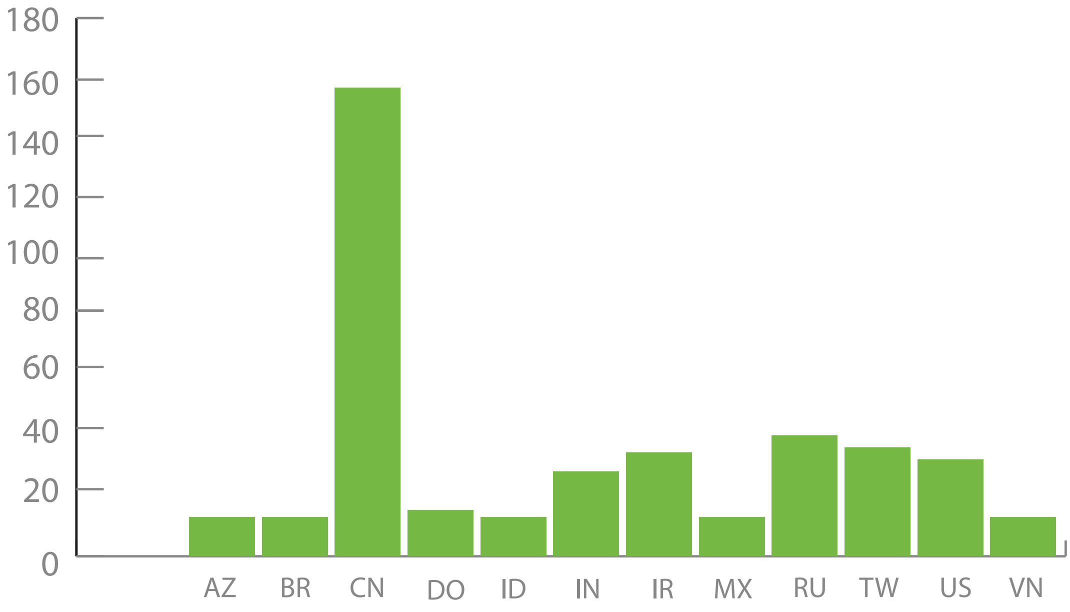


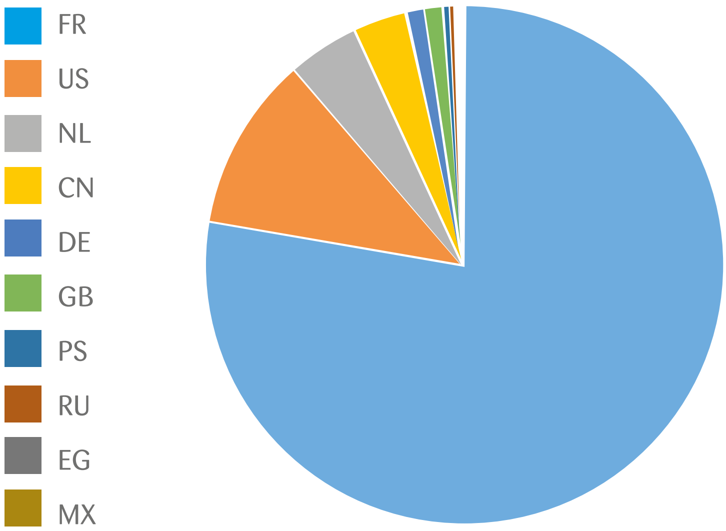
Figure 6: Attack distribution over 24 hours

Most successful attacker per country

By far, China had more successful sessions that any other country.



Even though most of attack seems to originate from French IPs, the attackers in this case were the least successful. It appears that the attacks executed from Chinese IPs were far more successful that attacks that originated from France.



How can Nettitude help?

A well thought out strategy should be in place for ensuring that VoIP services are not disrupted.

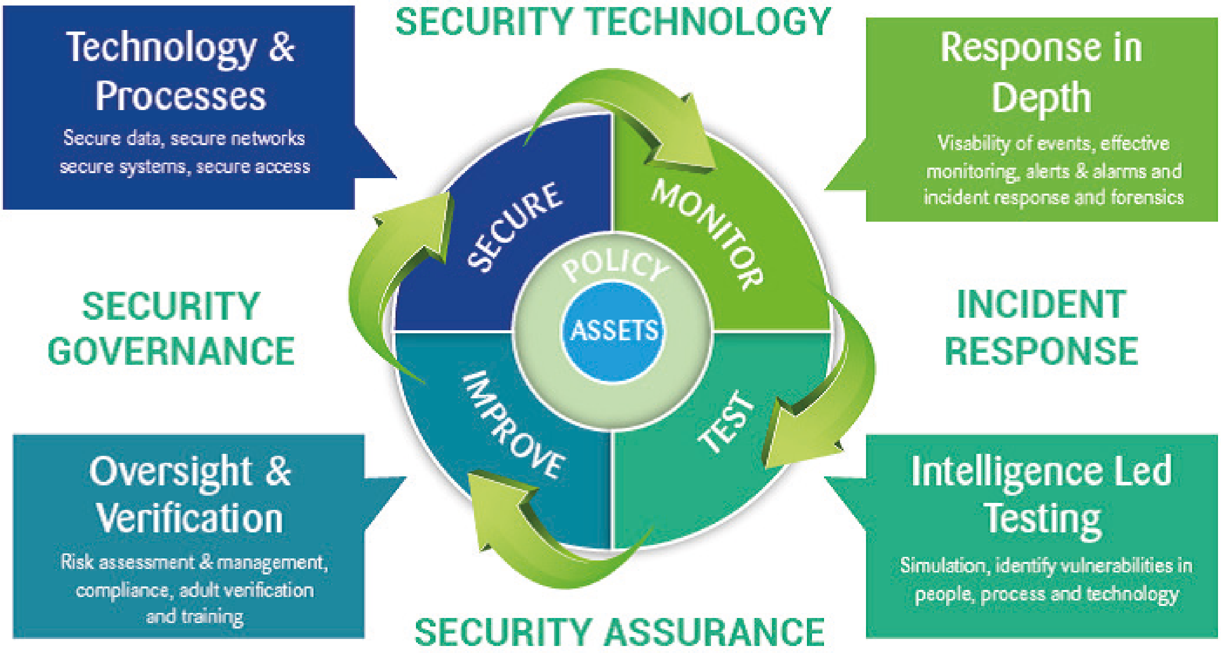
Statistics show that attackers operate when IT staff are likely to be away from their services. It is therefore important to have 24/7 monitoring system that will allow attacks to be detected and mitigated in real time. This is exactly what Nettitude offers in the managed service Threat2Alert (www.threat2alert.com).

Further to an efficient monitoring systems, Nettitude has gathered and continues to gather intelligence about VoIP malicious users, their respective tools and techniques. Such intelligence will be invaluable in protecting against know offenders and their techniques, whilst putting in place mitigation strategies for unknown actors.

Before applying any security, understanding the VoIP environment is paramount. This will help to understand the nature of the environment and its specific threats.

Nettitude has a team of technology specialists that can help identify the type of technology that would be suitable for specific environments.

360^{o} CYBER SECURITY


Technology & Processes
Secure data, secure networks secure systems, secure access
SECURITY TECHNOLOGY
Response in Depth
Visability of events, effective monitoring, alerts & alarms and incident response and forensics
SECURITY GOVERNANCE
SECURE
MONITOR
POLICY
ASSETS
IMPROVE
TEST
INCIDENT RESPONSE
Oversight & Verification
Risk assessment & management, compliance, adult verification and training
Intelligence Led Testing
Simulation, identify vulnerabilities in people, process and technology
SECURITY ASSURANCE

A holistic approach is very important in protecting against any cyber-attacks. The attackers might be awake when you are fast asleep. **GET PROTECTED NOW!**