THREATNIX

PURGE YOUR THREATS

THREAT REPORT 2018, NEPAL

Disclaimer

All information included in this document are intended for creating awareness regarding security issues rather than to encourage exploitation of the discovered shortcomings. We encourage every security researcher to notify the respective party regarding any security vulnerability they come across, so as to foster a culture of responsible disclosure and to create a cyber secure Nepal. Threat Nix is not liable for any misuse of information provided in this report which may or may not allow unauthorized access to systems.

During the course of this research, a number of publicly accessible hosts, devices and domains were analyzed and tested. This only represents a sample size and helps us create a bigger picture of the condition of Nepali cyberspace, and as such we cannot guarantee that our tests and report have encompassed all existing devices in Nepal, both publicly accessible or otherwise.

About Us

ThreatNix is a tight knit group of experienced security professionals who are committed to providing competent cybersecurity solutions that adhere to international standards. Our team of security experts deliver unbiased guidance and solutions before attacks become disruptions and financial hardships. We pride ourselves in providing the level of expertise that not only will help organizations identify vulnerabilities and areas of improvement but will also guide them on best practices to correct those vulnerabilities.

Our mission is to bring a paradigm shift in how cybersecurity is strategically and holistically addressed for organizations around the world. We strive to focus all our collective efforts on one single thing - be the first choice for all your cybersecurity needs. We intend to build a global culture of defending against cybercrime and are confident that our dedication towards it will drive the solutions which will ultimately provide state-of-the-art security for our clients.

Table of Contents

Table of Figures

Foreword

As in the previous year we have continued in our effort to assess the state of security of Nepali cyberspace. With ever increasing attempts of cyber-attacks and cyber warfare emerging as the new norm, it is essential to be more vigilant of our cyberspace. With more and more parts of administration and governance being digitized, we should put the utmost attention to security and making sure that cyber-attacks of any scale, small to large, cannot cripple the overall administrative functionality.

While continuing with the efforts of the past year by analyzing the publicly accessible devices and websites for lack of security and misconfigurations that can be used to exploit them, we have also attempted to make the report even more comprehensive. In this attempt, we have broadened the sample size for analysis, and opted to scan complete Nepali IP block where doing so was practical. Furthermore, this year we have also expanded our test cases and tested for increased number of misconfigurations and vulnerabilities. In a new addition, this year we have also collected credentials dumps of various data breaches and searched for emails of .np ccTLD and well-known Nepali corporate domains within these dumps. This has provided us an insight of how international data breaches affect Nepali users and organizations. This year, we also scanned Nepali websites to see if they were being used for malicious purpose like phishing and malware distribution and found a sizable number being used for such purposes.

To get a better understanding of the trajectory of cybersecurity in Nepal, we have compared this year's findings with that of the last year. To our dismay there is no clear indication of overall improvement in security implementation and awareness. While there is a notable improvement seen within some aspects of security, some negative trends were also observed. This indicates that the improvements observed are not the result of better security practices. Our research in the past had given us a positive sign about the security status as, it was not as bad as we expected it to be. Similarly, we were expecting to see an overall improvement in security this time but failed to find any clear indication of such improvement.

We hope this report will find its way to policy makers and security administrators and will help them in better understanding the status of security. With this we expect this report to be a force for change and improve the security status of Nepali cyberspace in order to create a cyber-secure Nepal.

Introduction

The year 2018 has been a global wake up call to address the cyber threat landscape. From resurgence of destructive ransomware, IoT botnets, data breaches and mobile malware to sophisticated multi-vector attacks, it's clear we are witnessing an inflection point and a transition to the fifth generation of cyber-attacks With each passing year, not only has the sheer volume of threats increased, but the threat landscape has become more diverse, with attackers working harder to discover new avenues of attack and cover their tracks while doing so.

The World Economic Forum recently placed cyber-attacks as one of the top three global risks for 2018 [1]. Data breaches took center stage last year, with shocking revelations made by governments and renowned business enterprises like Facebook, Marriott, Google about data compromised of millions of users. This took the world by storm and raised concerns about cyber security.

In the midst of myriad of constantly evolving threat landscape, it is critical that we define, assess and implement new pathways for cyber security. This report not only focuses on simply providing an assessment on the rise or fall of a particular threat but also contemplates on overall cyber security posture of Nepal and highlights the need to prepare for cyber-attacks by implementing necessary security measures.

Top Cyber Security Incidents Worldwide (2018)

Marriott Data Breach

On September 10, 2018, Marriott International, an American multinational hospitality company, acknowledged a data breach affecting 500 million customers who made a reservation at Starwood property since 2014. Over 325 million records in the database contained names, birthdates, physical addresses, email addresses, passport numbers, travel information, and Starwood rewards information. Reports have increasingly indicated that state-sponsored Chinese hackers were behind the attack, though this attribution has not been officially confirmed. The stolen data would be an espionage bonanza for government hackers.

Source: https://blog.avast.com/security-news-starwood-hotels-breaches

Aadhar Security Breach

In 2018, 1.1 billion records were compromised in Aadhar card breach incident, including name, address and other Personally Identifiable Information (PII). The report of breach was first disclosed in January 2018 which claimed that access to any Aadhar card holder's details could be purchased over the Internet. It was followed by several similar incidents of Aadhar card data leaks caused by faulty API of Indian government websites. Reports even asserted that a version of the enrolment software had been manipulated to let individuals generate Aadhaar numbers without submitting biometric data and illegally access the UIDAI's database.

Source: https://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html

Facebook

Cambridge Analytica

In March 2018, it was reported that Facebook profiles of 50 million users were harvested without their permission via an app that scraped details about people's personalities, social networks, and engagement on the platform by Cambridge Analytica. The number was later revised as many as 87 million user profiles. The breach allowed the company to exploit the private social media activity of a huge swath of the American electorate, developing techniques that underpinned its work on President Trump's campaign in 2016. After the breach was disclosed in public, Facebook was fined £500,000, the maximum amount possible, for its part in the scandal.

Source: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

‘View as’ feature

In September 2018, 50 million Facebook users were automatically logged out of their Facebook accounts due to an attack via the Facebook 'View as' feature. The hackers began by exploiting the video uploading feature and eventually chained this together with a weakness in the “View As” feature. During this process a user token was generated when it wasn’t intended to happen for the one subject to “view as” and this appeared in the HTML code. From there the hackers gained access to the user accounts and automated their attack which eventually resulted in an activity spike. This caught Facebook’s attention and they responded swiftly to stop the breach. In total, there were 3 bugs that the malicious actors were able to chain together to gain access to user tokens. When Facebook was aware of this, it forced log out to reset tokens for 50 million users and an additional 40 million who were potentially affected.

Source: https://newsroom.fb.com/news/2018/09/security-update/

Google+

In March 2018, Google discovered that a bug in Google+ API had been allowing third-party app developers to access the data not just of users who had granted permission but also of their friends. Within three months, Google again spotted a security issue that exposed data of 52.5 million users. The bug in Google's developer platform on its Google Plus social network left information like user's name, email address, occupation, gender and age, vulnerable to data breach. Shortly after the incident, Google announced that it will shut down consumer access to Google+ and improve privacy protections for third party applications.

Source: https://www.blog.google/technology/safety-security/project-strobe/

Quora Data Breach

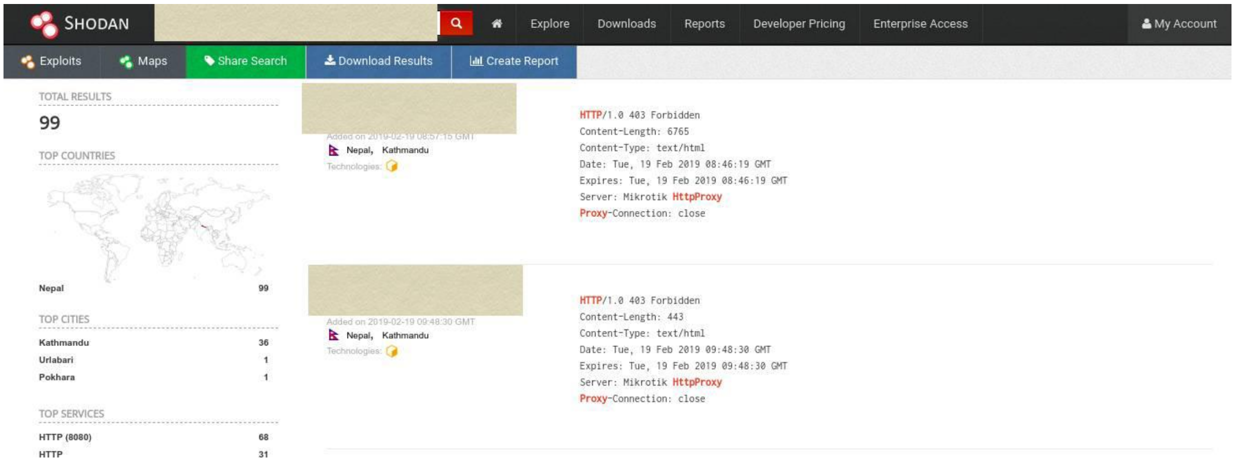
In December 2018, Quora revealed that a malicious third party gained access to their systems and swiped the account data of approximately 100 million users. Compromised information includes cryptographically protected passwords, full names, email addresses, data imported from linked networks, and a variety of non-public content and actions, including direct messages, answer requests, and downvotes. The breached data also included public content and actions, such as questions, answers, comments, and upvotes. Though no financial information is attached to Quora accounts, there’s a ton of personal and social information available for each account.

Source: https://blog.quora.com/Quora-Security-Update

Mikrotik Routers Compromised to Inject Cryptojacking Malware

A cryptojacking malware has been targeting vulnerable Mikrotik Routers worldwide [2]. In case of Nepal, we found 88 infected routers looking strictly at Coinhive alone. However, Coinhive isn't the only type of Cryptominer that these malwares are using.

These MikroTik routers are being compromised by miscreants exploiting CVE-2018-14847, a critical vulnerability that affects all versions of RouterOS through 6.42. A patch was issued earlier this year by MikroTik, however the latest statistics reveal many device owners and network operators have chosen not to apply it.



[redacted]

TOTAL RESULTS

99

TOP COUNTRIES

Nepal	99

TOP CITIES

Kathmandu	36
Urlabari	1
Pokhara	1

TOP SERVICES

HTTP (8080)	68
HTTP	31

[redacted]

Nepal, Kathmandu

Technologies:

```
HTTP/1.0 403 Forbidden
Content-Length: 6765
Content-Type: text/html
Date: Tue, 19 Feb 2019 08:46:19 GMT
Expires: Tue, 19 Feb 2019 08:46:19 GMT
Server: Mikrotik HttpProxy
Proxy-Connection: close
```

[redacted]

Added on 2019-02-19 09:48:30 GMT

Nepal, Kathmandu

Technologies:

```
HTTP/1.0 403 Forbidden
Content-Length: 443
Content-Type: text/html
Date: Tue, 19 Feb 2019 09:48:30 GMT
Expires: Tue, 19 Feb 2019 09:48:30 GMT
Server: Mikrotik HttpProxy
Proxy-Connection: close
```

Figure 1: Vulnerable Mikrotik Routers

We have categorized the results on the basis of organizations in the figure presented below:

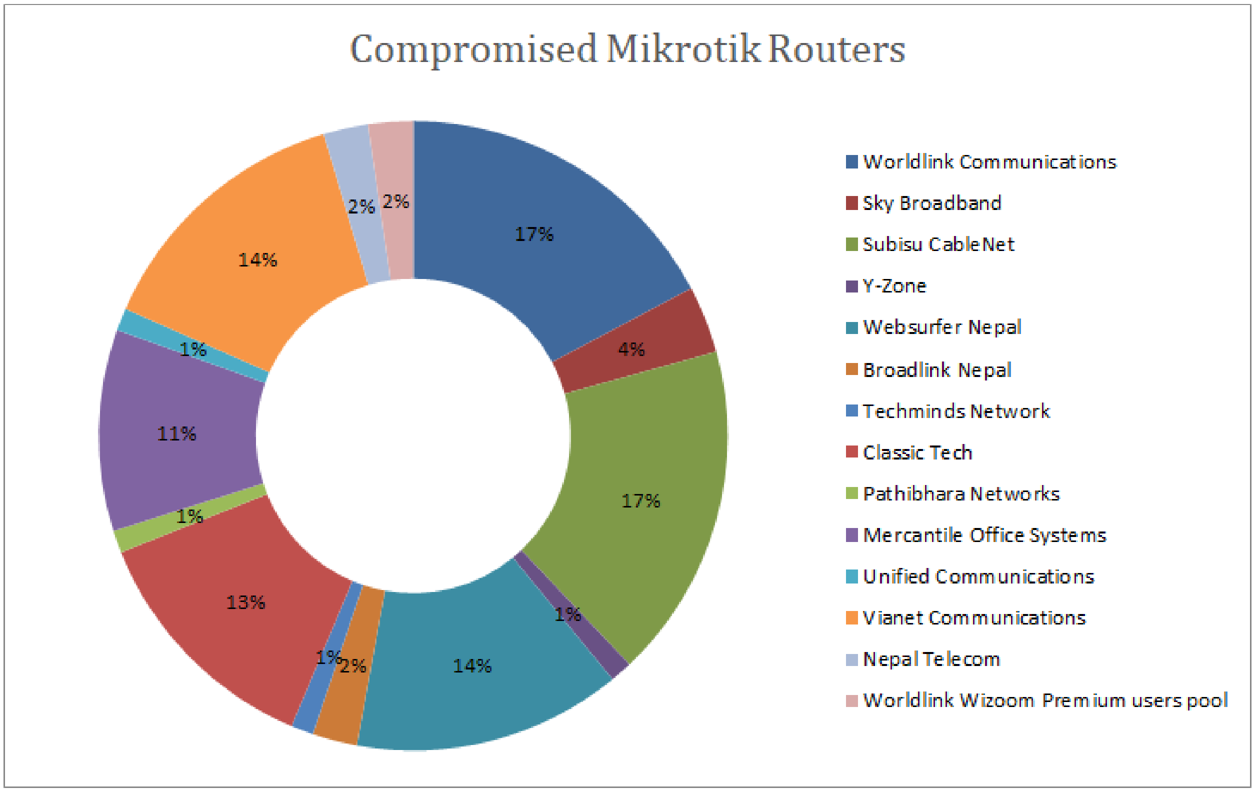


Figure 2: Compromised Mikrotik Routers: By Organization

Statistics of Websites in Nepal

The data and statistics have been collected performing various tests on the total of 54589 unique .np domains. The domains were collected using several reconnaissance methods along with the help of wordlists we gathered from various sources. Combined with domain names collected from other sources, we ran a test which gave us the following result:

- Publicly exposed configuration file with password on it
- Publicly exposed .git
- Publicly exposed Server Status
- Publicly exposed phpinfo
- Publicly exposed SSH key
- Misconfigured CORS
- Directory Listing on '/'
- Default Server Pages
- 'Hacked by' like titles
- Php 5.x

We also tested for SSL implementation within these domains. Among the 54589 domains we found only 5915 had implemented SSL and 33838 were confirmed to have no SSL implementation. We also noted misconfigurations in the SSL implemented hosts which resulted in vulnerabilities like Heartbleed. With SSL being freely provided by services like Let's Encrypt, it is unexpected to see such large majority of websites not implementing SSL and taking the security of user data with such negligence.

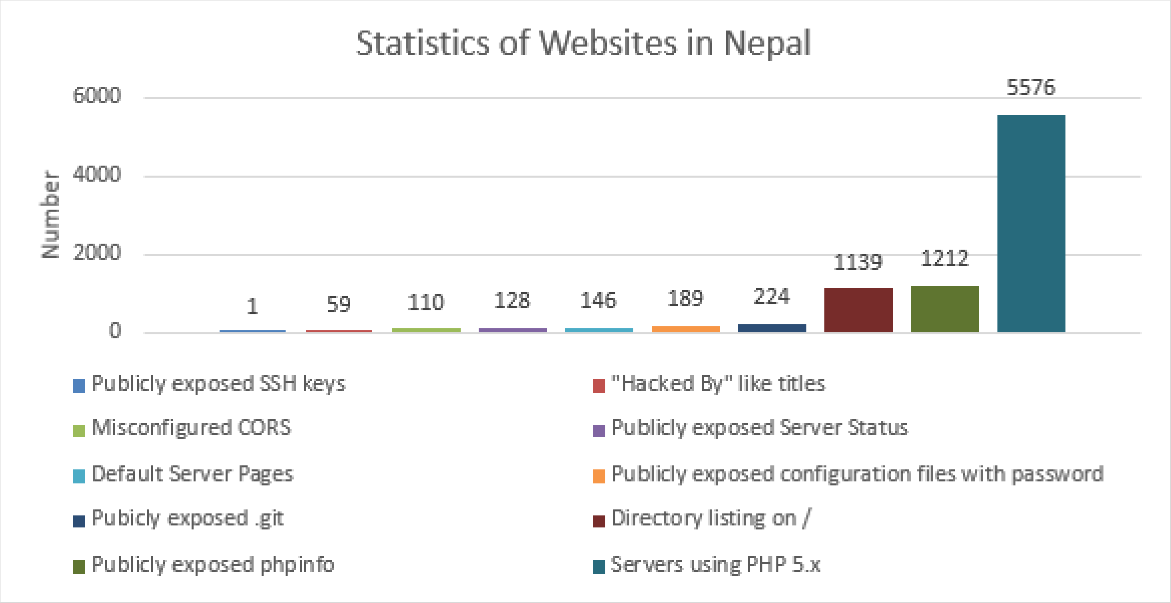


Figure 3: Statistics of Websites in Nepal

Publicly exposed configuration files with password

These are mostly web server configuration files that contain various settings along with passwords. These passwords and configurations might in some cases allow an attacker to obtain full access to the server. We discovered 189 websites exposing these configurations publicly.

Publicly exposed '.git'

The '.git' directory contains version control information to keep track of changes in source code. These directories might expose applications to unexpected catastrophes. There were 224 domains with publicly accessible '.git' directory that are leaking source code of application which in certain circumstances, can be leveraged to take full control of the server.

Publicly exposed Server Status

A web server's 'server-status' page allows server administrators to find out how well their servers are performing. This page exposes server information like CPU usage, server uptime, IP addresses, incoming request to the server etc. If anything, sensitive like API keys or session tokens are being sent to the server via URL, they are displayed on server status page. Such sensitive information may then be used to compromise the user or even the server. We found 128 domains exposing 'server-status'. Aside from 2 Tomcat servers, all of the others server exposing 'server-status' are Apache servers.

Publicly exposed phpinfo

Similar to server-status, 'phpinfo' is a debugging functionality intended to help administrators. This discloses complete information about php and its configuration. Attackers can leverage this information to use against the server. We found 1212 domains disclosing 'phpinfo'.

Publicly exposed SSH Key

SSH is used to remotely access a system through the internet. SSH keys can be used in servers to authenticate users without password. While public keys are meant to be public and causes no harm even if exposed, private keys shouldn't be exposed. We found a web server publicly exposing its private SSH key.

Misconfigured CORS

Cross Origin Resource Sharing (CORS) is a mechanism which allows client-side script hosted on one domain(origin) to read contents of another domain(origin). CORS, when improperly configured, allows attacker's site to access private information of logged in user from vulnerable application. 110 of the tested sites had misconfigured CORS. This means, if a user is logged in to these vulnerable sites visits attacker's site, attacker would be able to access private information of user from these sites.

Directory listing on /

Due to missing index pages in web server, whenever a user browses the site, files and directories in the web root directory is listed. This allows anyone to access possibly sensitive information like web configurations files, private documents and confidential information. We found 1139 servers with directory listing on /.

Default Server Pages

The best parameter to identify a default page is via title. We gathered 9 set of titles from IIS, nginx, JBoss, Bitnami, Ruby on Rails, Tomcat, Apache and GlassFish. This gave us 146 unique domains with default welcome page.

“Hacked by” like titles

Since we were already looking for default titles, we expanded our search to look for titles that are generally found in hacked or defaced web pages. We went through zone-h archive and took note of titles of already defaced pages. The small set of titles we checked for revealed 59 unique domains which were, in fact, all hacked and defaced.

PHP 5.x

PHP version 5 reached its end-of-life and stopped receiving security updates on January 1, 2019. As per our analysis, we found that 5576 websites were still using PHP 5.x, which already have multiple vulnerabilities as listed in CVEdetails [4]. These websites are now left in a precarious position as no security patches will be available for the current vulnerabilities as well as the critical vulnerabilities that will definitely be discovered over time.

Moreover, vulnerabilities in PHP Running Version Prior to 5.3.26 is a high-risk vulnerability that is frequently found on networks around the world. This issue has been around since at least 1990 but has proven either difficult to detect, difficult to resolve or prone to being overlooked entirely.[5]

Statistics of Corporate Websites

It is generally expected of corporations and business organisations to give considerations to their security. Corporations have a greater incentive to keep their data secured as often times, such information can be used for financial gains by malicious actors. So, to assess the security of corporations, we sampled 165 corporate domains and found them to have following security misconfigurations.

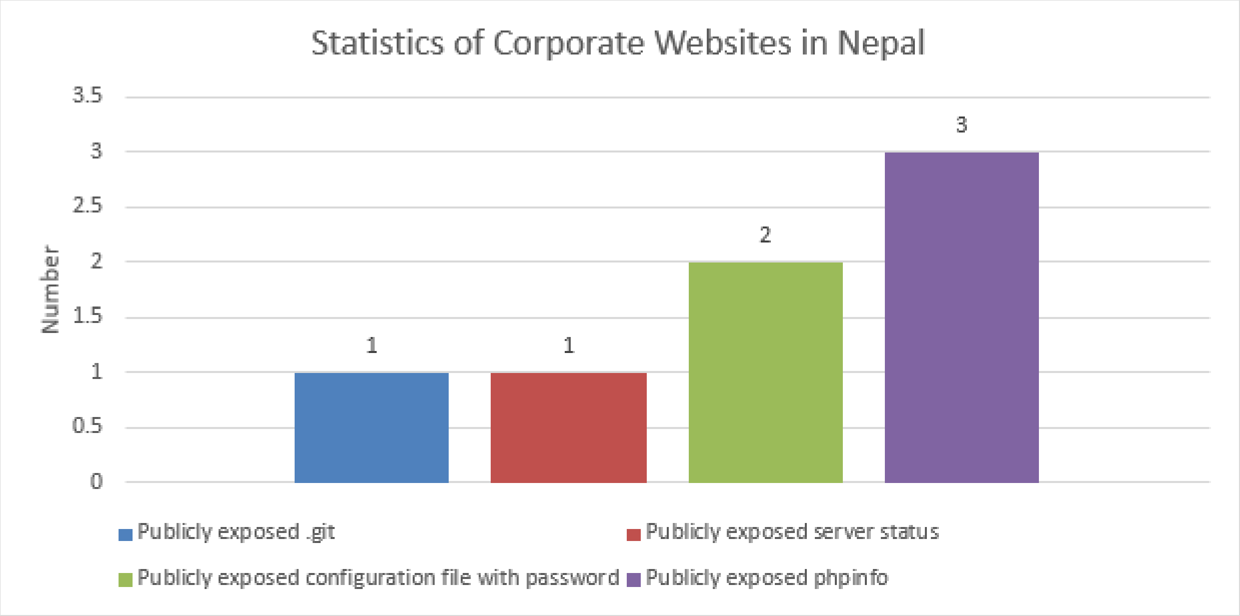


Figure 4: Statistics of Corporate Websites in Nepal

These files/directories contain extremely sensitive information and shouldn't be available to public. In cases of exposed configuration files with password and exposed ".git", the information disclosed can be used to gain complete control of the web server and thus compromise the corporate network. The attackers can then use the compromised servers to extract information which can be used to deal severe financial loss to the organisation.

Hacked and Defaced Websites

Website defacement is unauthorized access on web page or entire website; mutilating its structure. Typically, a defaced website would have undergone unauthorized changes to its appearance, often through altered, or totally replaced company logos, text content, or web pages in their entirety. Since web defacement is relatively easier to carry out than other forms of cyber-attacks, such incidents are quite prevalent.

While trying to determine the prevalence of act of defacement in Nepal, we conducted a research on defaced Nepali websites with the help of “Zone-H”. “Zone-H” maintains an archive of defaced websites. Once a defaced website is submitted to Zone-H, it is mirrored on the Zone-H servers, which is moderated by the Zone-H staff to verify the credibility of defacement.

There were a total of **‘434’** Nepali websites defaced in 2018. The following bar graph presents a categorized view of different TLDs defaced during 2018:

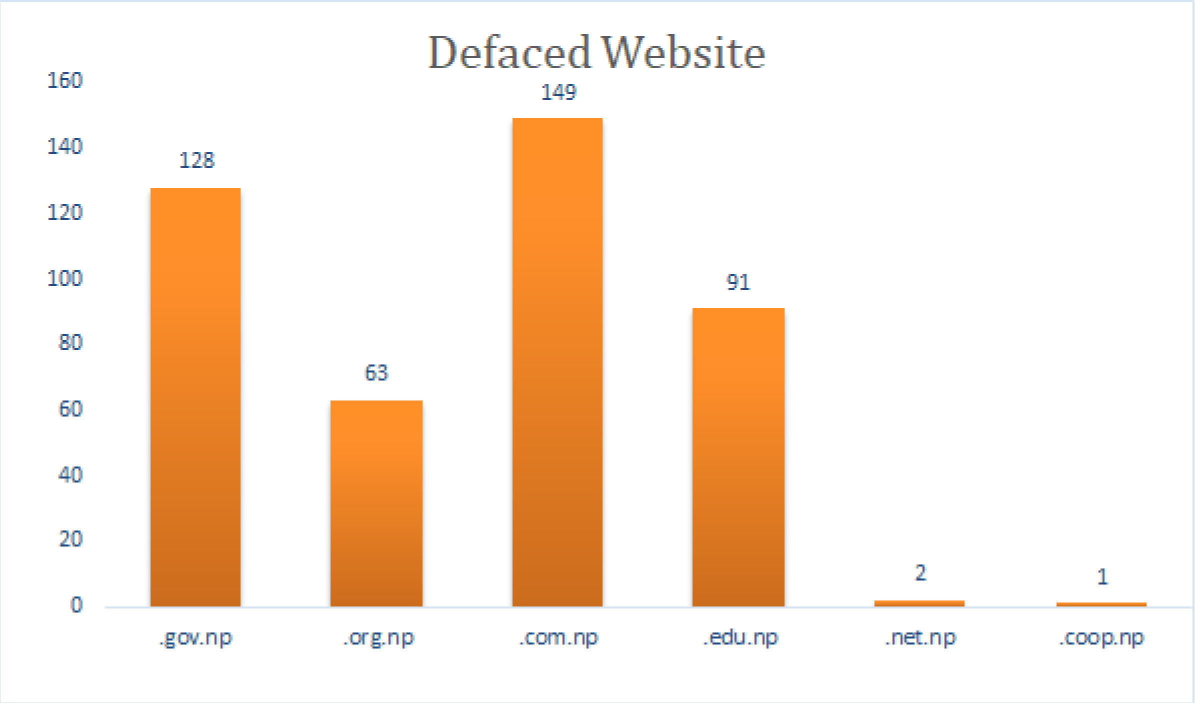


Figure 5: Defaced Websites of Nepal in 2018

While doing research on defaced websites, we observed that 329 websites were victim of mass defacement. It's not uncommon to find multiple sites being hosted on the same server. The real issue is with badly configured access control policies which allow one account to access files outside of their assigned space. The following bar graph presents identical categorized view of different TLDs found in mass defacement:

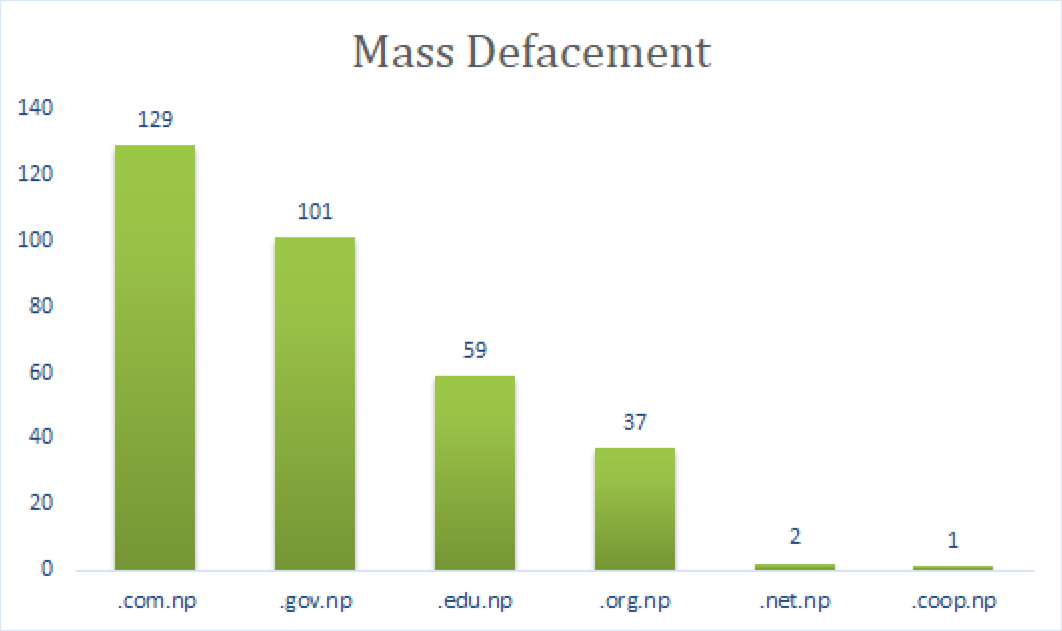


Figure 6: Websites victim of Mass Defacement in 2018

Earlier at the end of 2017, during our research for Threat Report 2017[3], we found out 756 Nepali websites were defaced where 595 were victims of mass defacement. While comparing the findings of this year to that of last year, we saw an interesting shift in the number of defaced and mass defaced websites. In 2018, the number decreased to 434 defaced websites and 329 websites that had been mass defaced. While this result projects a positive trend towards website security in Nepal but we still have to see if this is due to improvement in security or due to reduced defacement attempts overall. Still, this decrease in the number of defacements is a hopeful indication of growing security awareness.

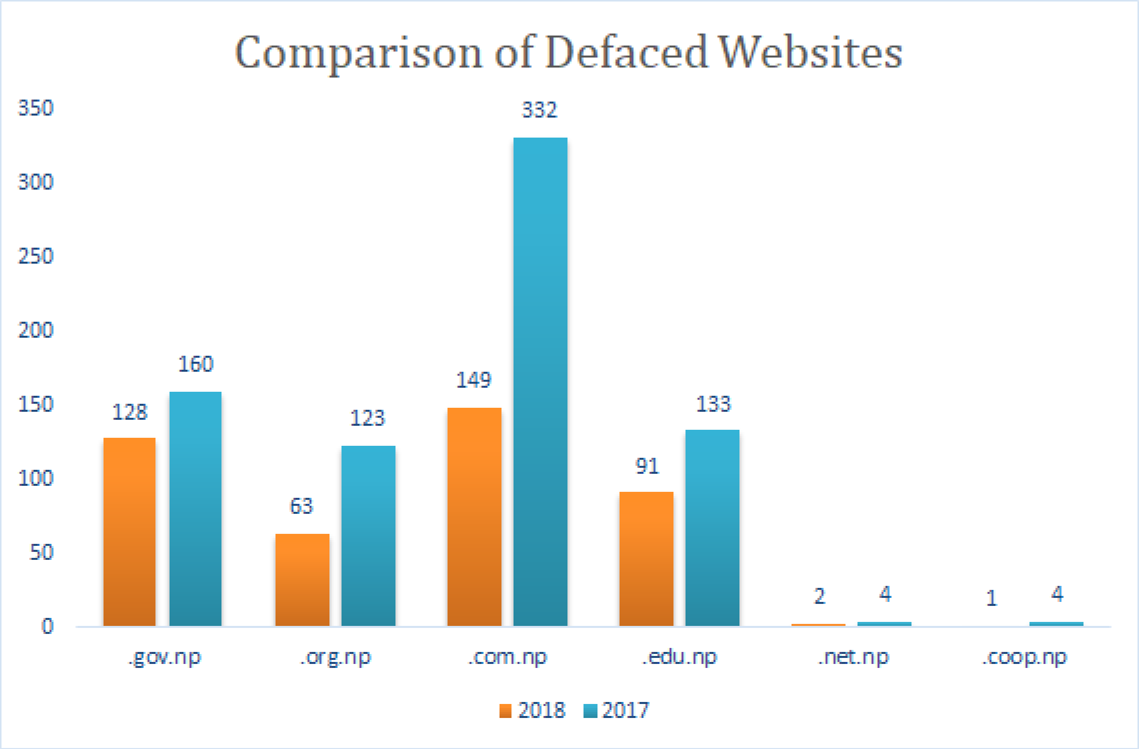


Figure 7: Comparison of Defaced Websites in 2017 and 2018

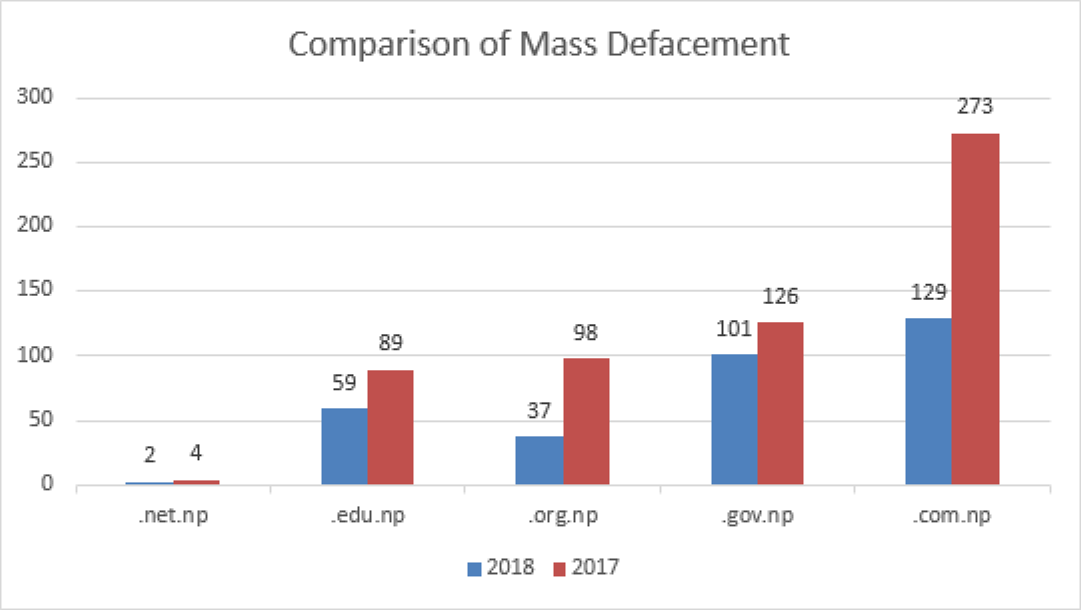


Figure 8: Comparison of Mass Defacement in 2017 and 2018

Hacked Devices

Almost all devices and services have some weakness that an attacker can exploit to compromise the device. These devices when made publicly reachable on the Internet become prone to attacks and are constantly compromised. When we looked for “hacked” devices in Shodan within Nepal, we found 35 devices which were indeed hacked. We have categorized our findings grouped by organizations as shown in the figure below.

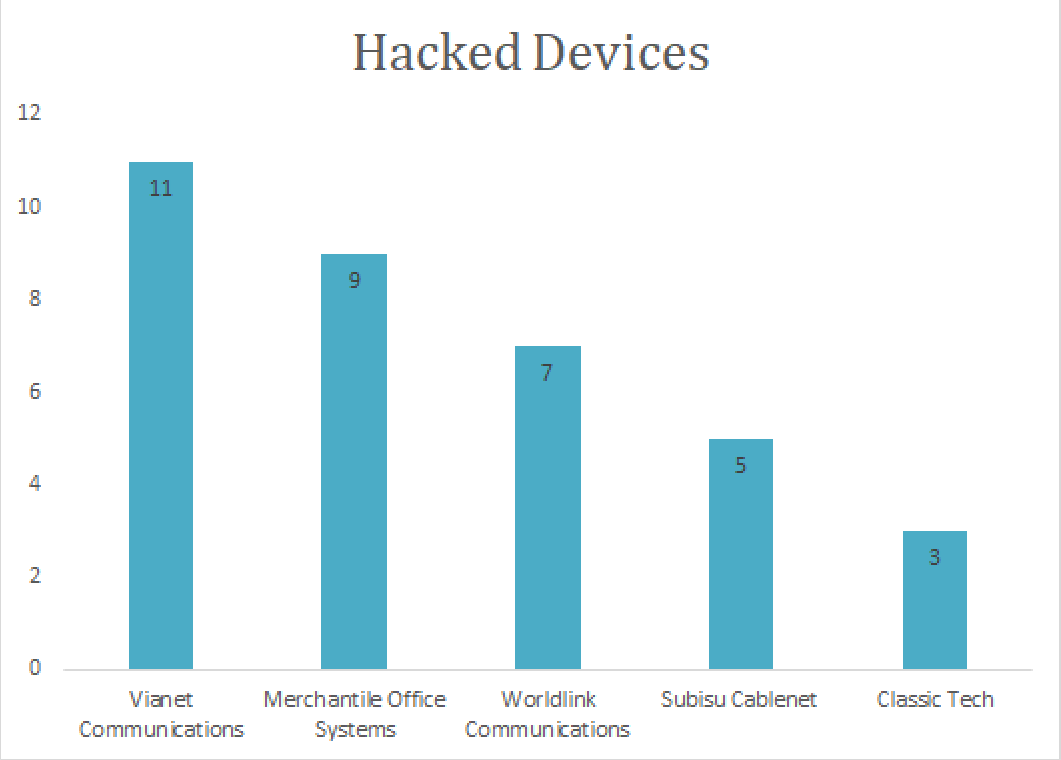


Figure 9: Hacked Devices: By organization

We found 9 Ubiquiti Network Devices that were hacked and have their hostnames changed revealing what led to its compromise. One of the device’s name was changed to ‘HACKED-ROUTER-HELP-SOS-HAD-DUPE-PASSWORD’, which means the device was using a duplicate password of some vulnerable device.

Other 6 devices’ name were changed to ‘HACKED-ROUTER-HELP-SOS-VULN-EDB-39701’. The hacked routers have a very self-explanatory name, meaning the devices were vulnerable to AirOS 6.x - Arbitrary File Upload (EDB-ID: 39701) vulnerability.

Remaining 2 devices’ name were changed to HACKED-ROUTER-HELP-SOS-DEFAULT-PASSWORD which means the devices were using default passwords, making them an easy target to compromise.

Publicly Exposed Webcams

An insecure embedded device connected to the internet is a potential target for attacks, including CCTV systems. A quick Shodan search revealed 16 cameras that were exposed publicly, out of which 8 had default credentials, 3 had changed their password and 5 were throwing communication error during the test.

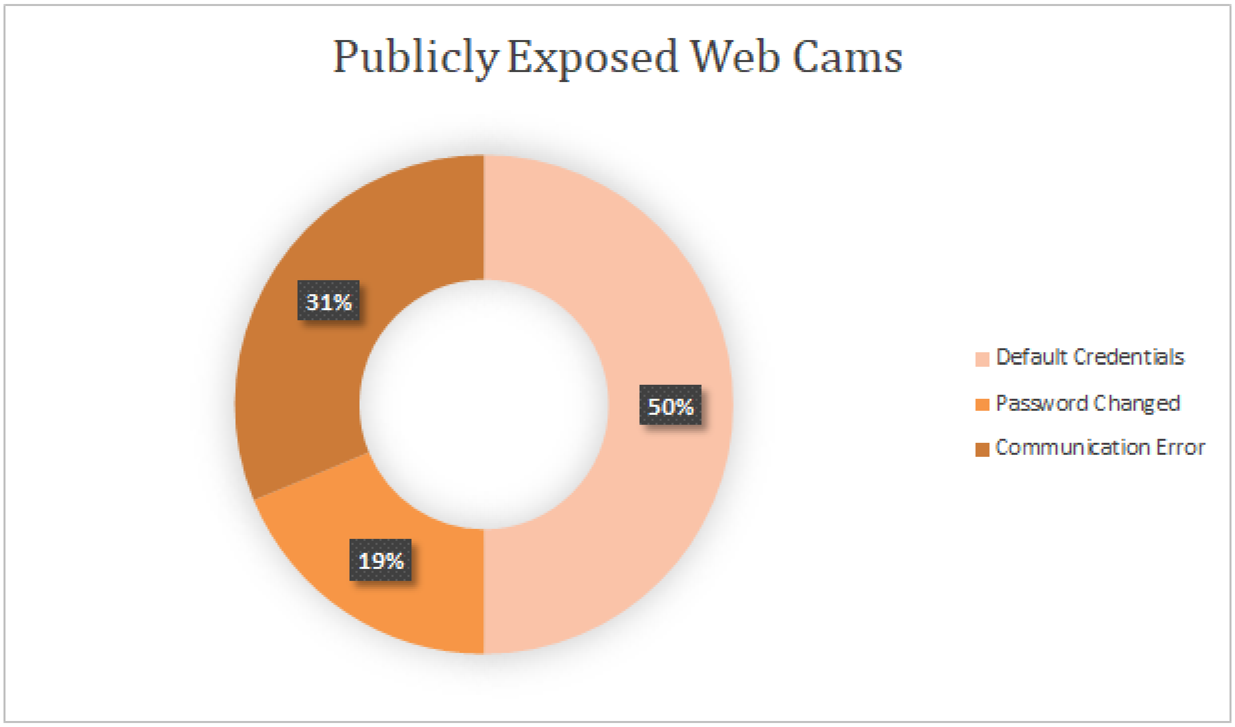


Figure 10: Publicly Exposed Web Cameras

Default Passwords

TP-LINK Devices

As per TP-LINK, “TP-Link is the world's #1 provider of consumer Wi-Fi networking devices, shipping products to over 120 countries and hundreds of millions of customers”. A quick Shodan search revealed a total of 279 TP-LINK devices in Nepal. Out of which 25 had default credentials, 98 had changed their password and 156 were throwing communication error during the time of testing.

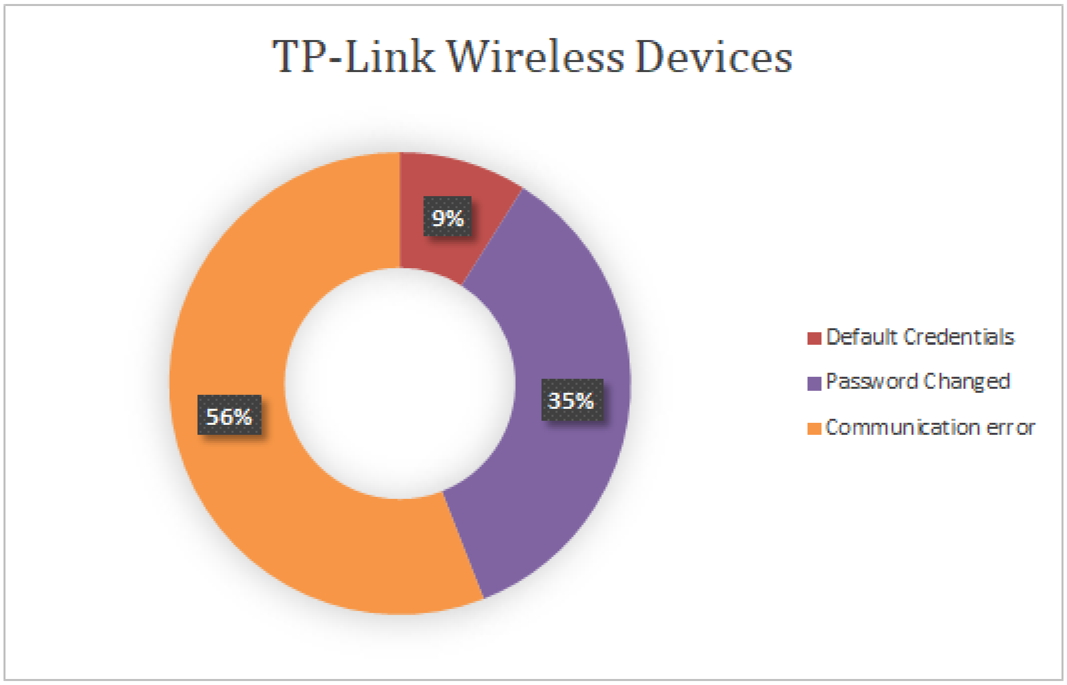


Figure 11: TP-Link Wireless Devices

We have categorized our findings of TP-Link devices used in Nepal on the basis of ISP through which they were connected to internet in the figure below:

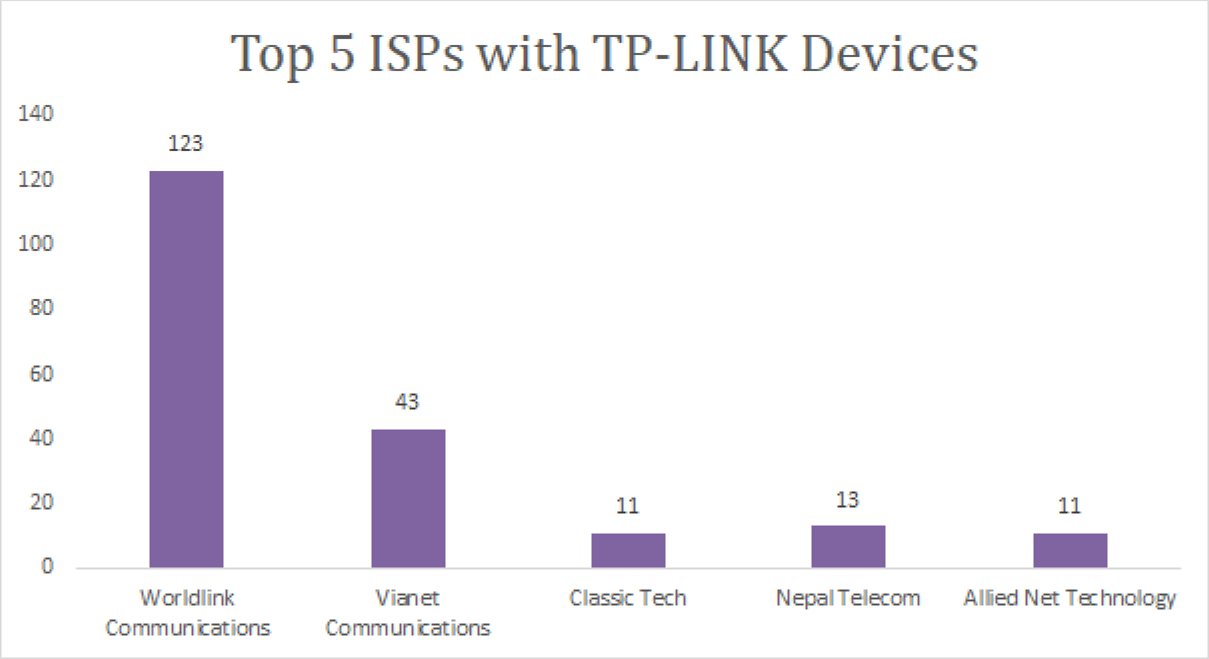


Figure 12: Top 5 ISPs with TP-Link Devices

WiMAX Devices

Wimax (Worldwide Interoperability for Microwave Access) is a family of wireless communication standards based on the IEEE 802.16 set of standards, which provides multiple physical layer (PHY) and Media Access Control (MAC) options. Nepal Telecom provides 4G WiMAX IEEE 802.16e service for broadband internet access. A quick Shodan search revealed 75 WiMAX devices in Nepal, out of which 12 devices still had default credentials.

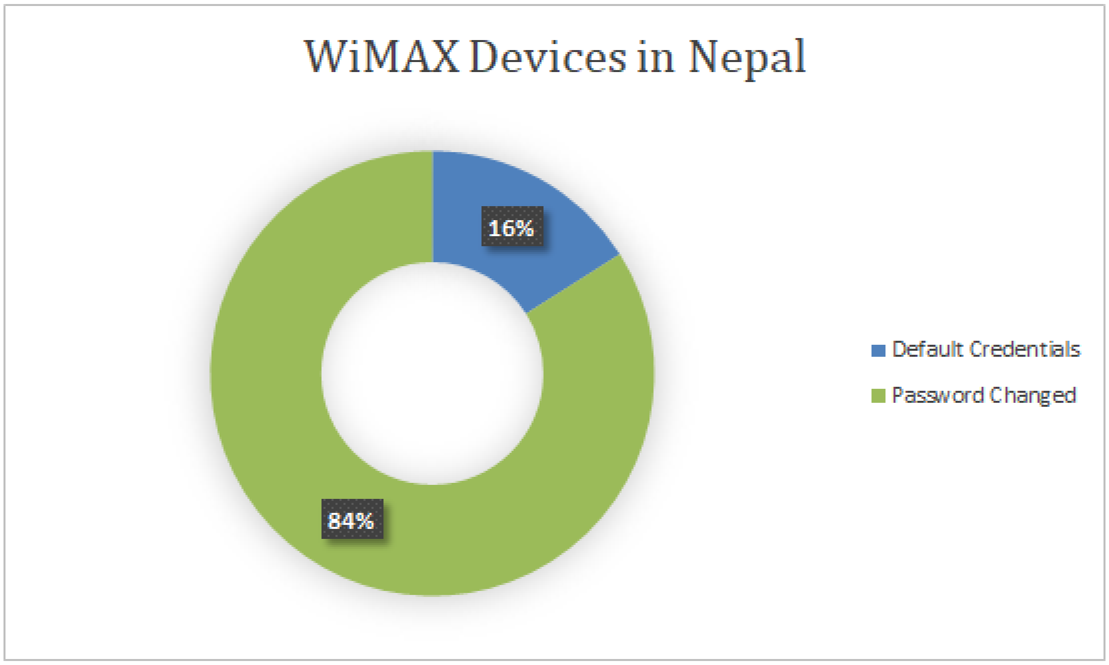


Figure 13: WiMAX Devices in Nepal

Other Generic Routers

A quick Shodan search revealed 100 other generic routers used in Nepal, out of which 70 devices still had default credentials.

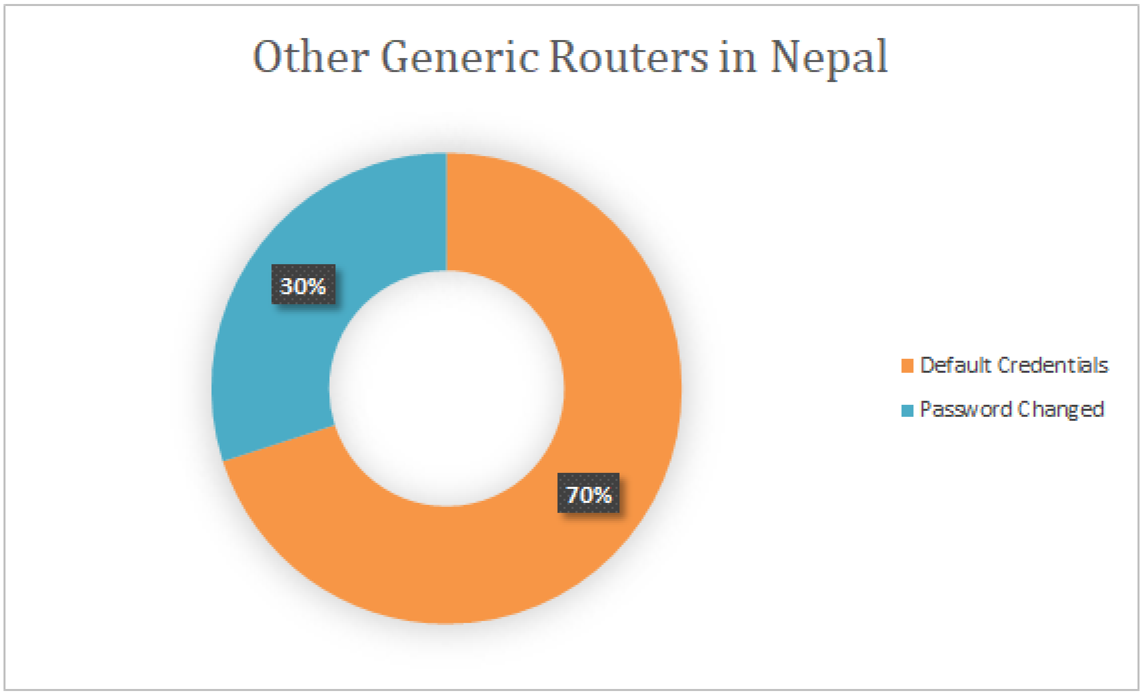


Figure 14: Other generic routers in Nepal

Password in Banner

We found a total of 17 devices with the password announced in their banner. Out of which 7 were unreachable during our test, 5 had changed their password and 5 were using the password announced in their banner.

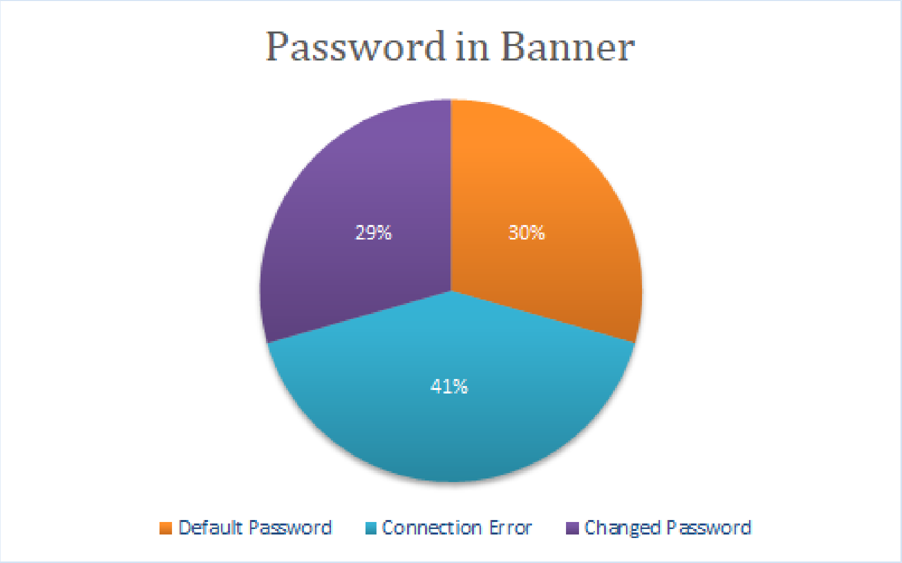


Figure 15: Password in Banner

In the figure below, we have presented the devices on the basis of organization that had password announced in their banner.

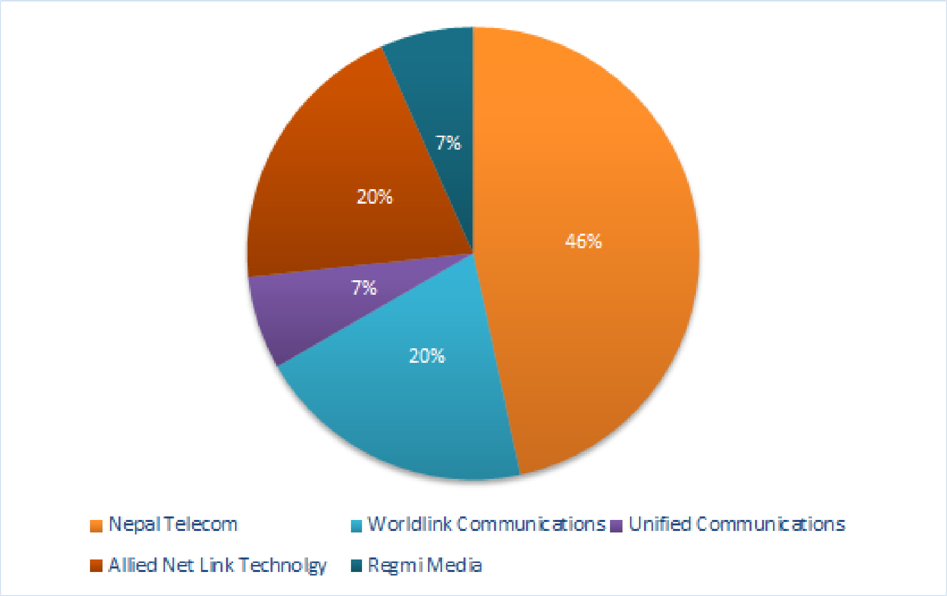


Figure 16: Devices with password announced in banner: By organization

Misconfigured Databases

During our research, we looked at one of the many corners of the internet that we tracked at expanse and found quite a few misconfigured database instances. Despite their popularity and large user base, one thing that is common in these instances is they are not security hardened for the public facing internet. The findings include databases with no authentications or with default credentials and instances that should not be publicly accessible at all.

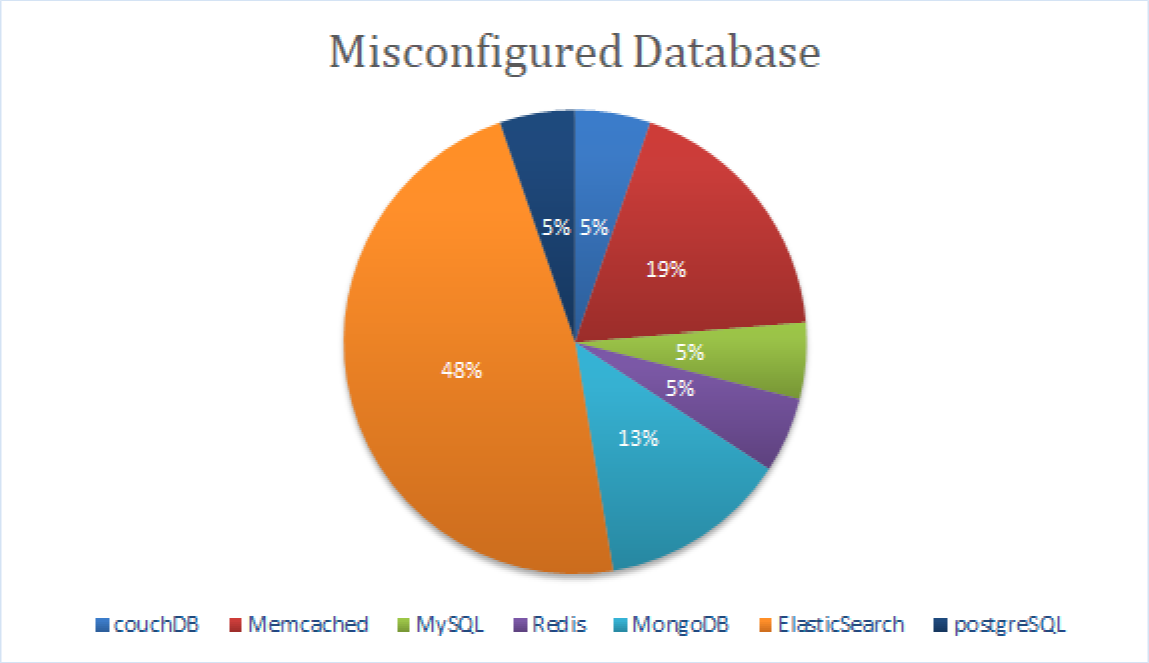


Figure 17: Misconfigured Database

Misconfigured Services

During our research, we found quite a few misconfigured services. Some of these services lack authentication and allow access to sensitive information to anyone on the Internet while they are meant to be used within a trusted internal network but have been made publicly accessible over the internet.

During our analysis, we found that several internal administration tools were publicly exposed, which leaks internal information to administrators and can easily lead to server compromise. FTP servers with anonymous login were exposed allowing anyone to access the files within these servers. Similarly, various IoT devices using IPMI (Intelligent Platform Management Interface) protocols connected to the internet were also exposed.

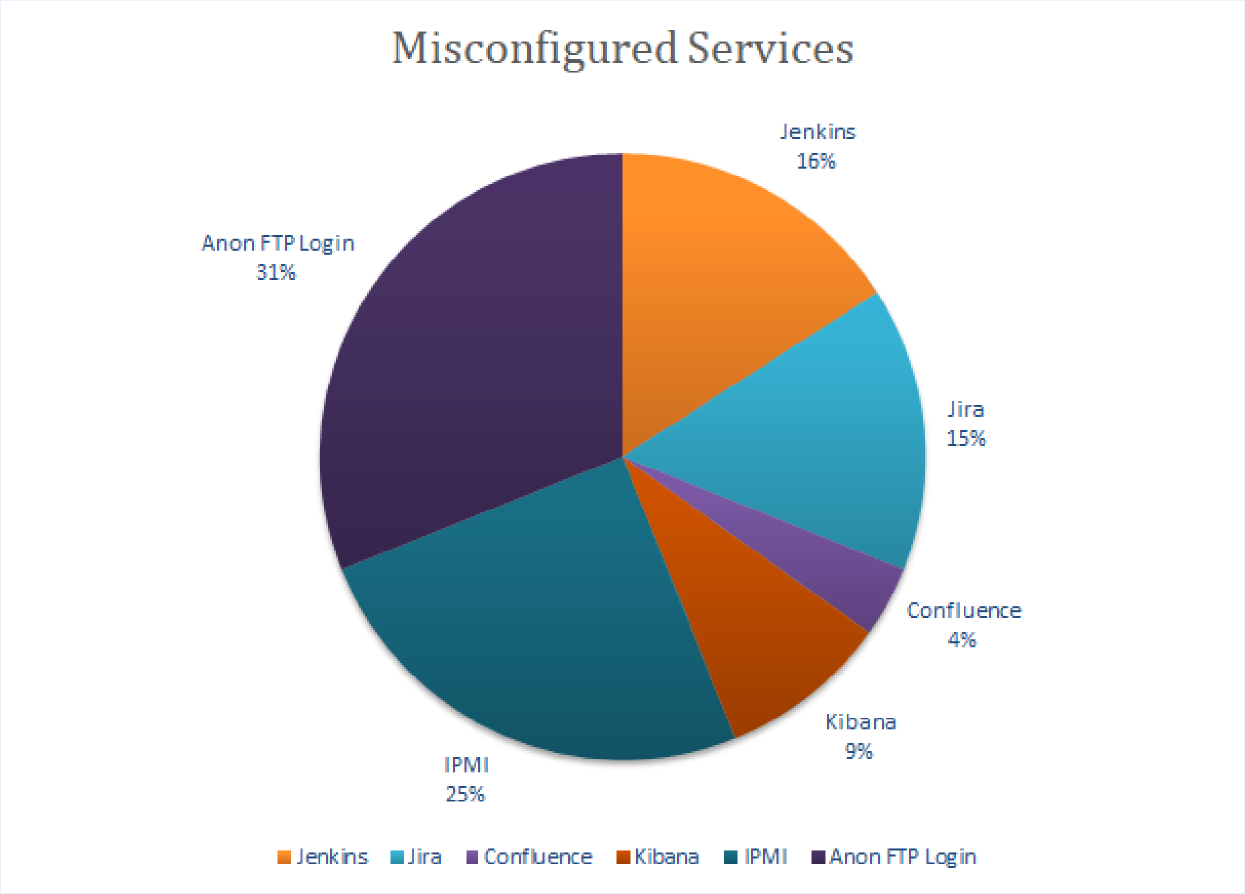


Figure 18: Misconfigured Services

Websites used for Malicious Purpose

Given its popularity and ubiquity, the internet attracts the attention of cybercriminals. Our analysis revealed that 222 websites are being used for malicious purposes in Nepal in 2018. We believe most of them are compromised and serving contents of hackers' choice without their owners knowing anything. Though, we cannot also deny the fact that it's a lucrative way of making some easy money. Out of 222, 213 were social engineering websites and 9 were malware distributing domains.

Social Engineering

The purpose of social engineering is always to elicit a wanted or beneficial response to some external stimuli. One thing that makes social engineering especially dangerous is that it relies on human error, rather than vulnerabilities in software and operating systems. Mistakes made by legitimate users are much less predictable, making them harder to identify and thwart than a malware-based intrusion.

Malware Distribution

Malware distribution via website is designed in such a way that it evades security software and performs malicious activities, such as gaining control of the victim’s computer, stealing the victim’s private information, launching denial-of-service (DDoS) attacks, and spamming.

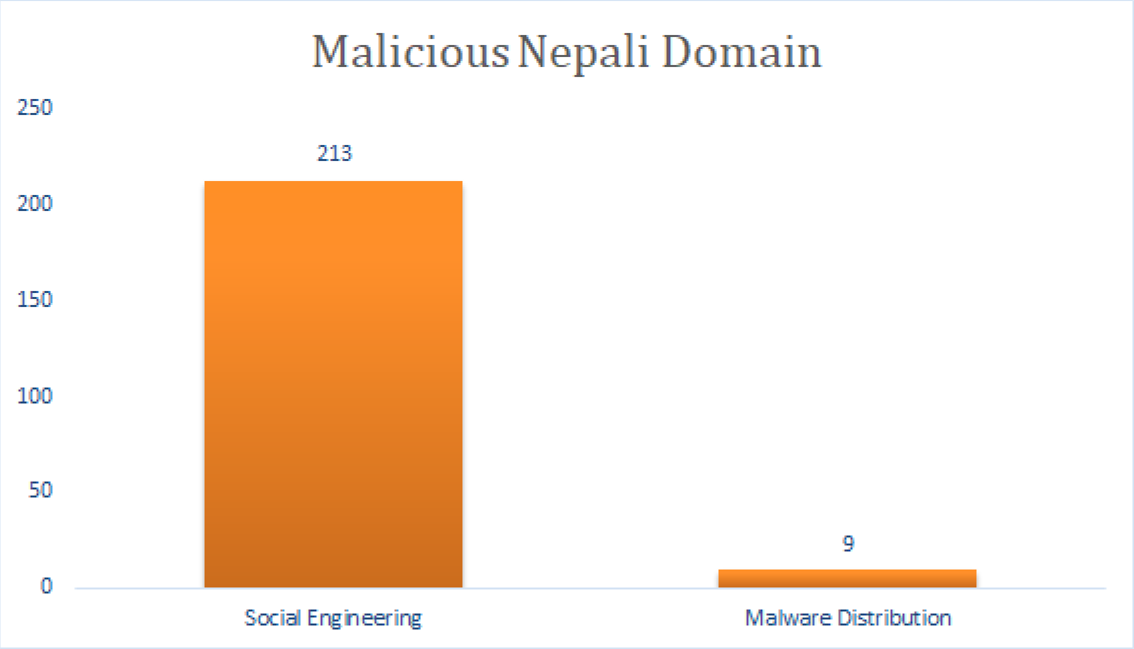


Figure 19: Nepali Websites used for Malicious Purposes

Data Breaches

We extended our research to account data breaches as well. We extracted emails from already breached datasets where we discovered a total of 8378 (.np) Nepali emails which are readily available for download and also contains plaintext passwords. It was shocking to see that a majority of emails we found were of corporate & financial institutions. The total number of breached emails associated with various banks of Nepal alone was 3299, this number contains 1082 emails belonging to banks with domain with Nepali ccTLD (i.e .np) and 2217 emails belonging to Nepali banks domains with other TLD (like .com).

When we looked at passwords found alongside these breaches, none of them looked strong enough and were mostly names, contact numbers, location or common passwords like 123456.

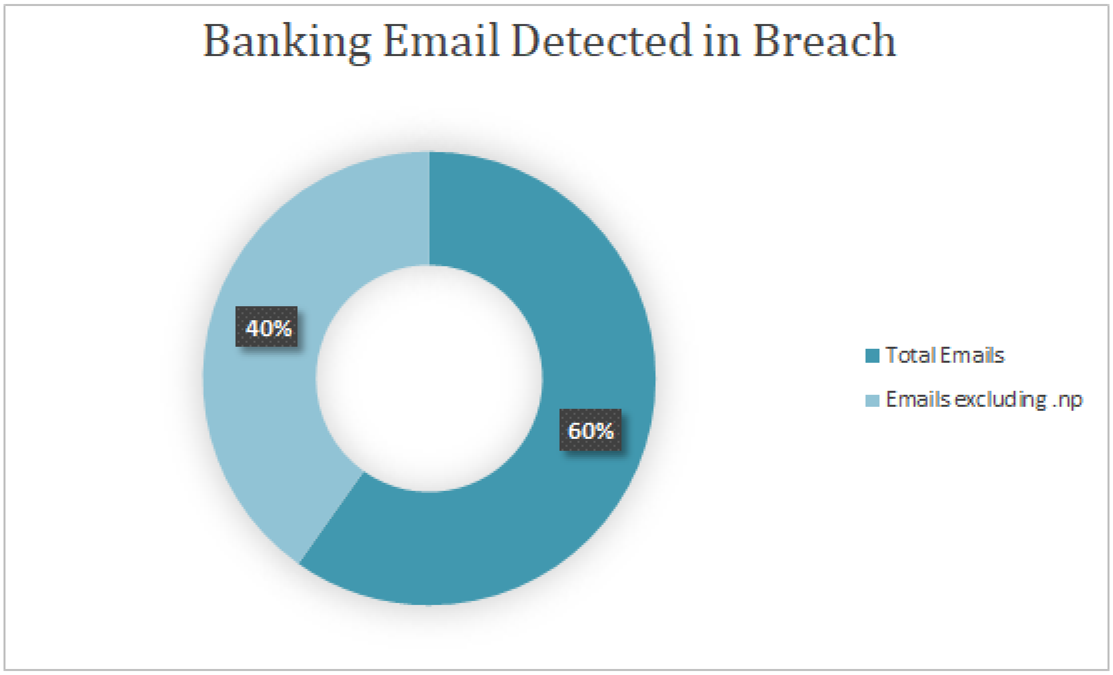


Figure 20: Banking Emails Detected in Breach

Government Emails in Data Breaches

We further extracted emails from government websites and checked if they have been in public data breaches using HaveIBeenPwned API. We were able to collect a total of 10141 unique email addresses from various government websites, out of which 1016 email addresses were found in multiple data breaches which also include emails from bodies like Nepal Police, Election Commission and alike. We also discovered many of these organisational emails being used to create personal profiles in various websites even adult sites like Adult Friend Finder.

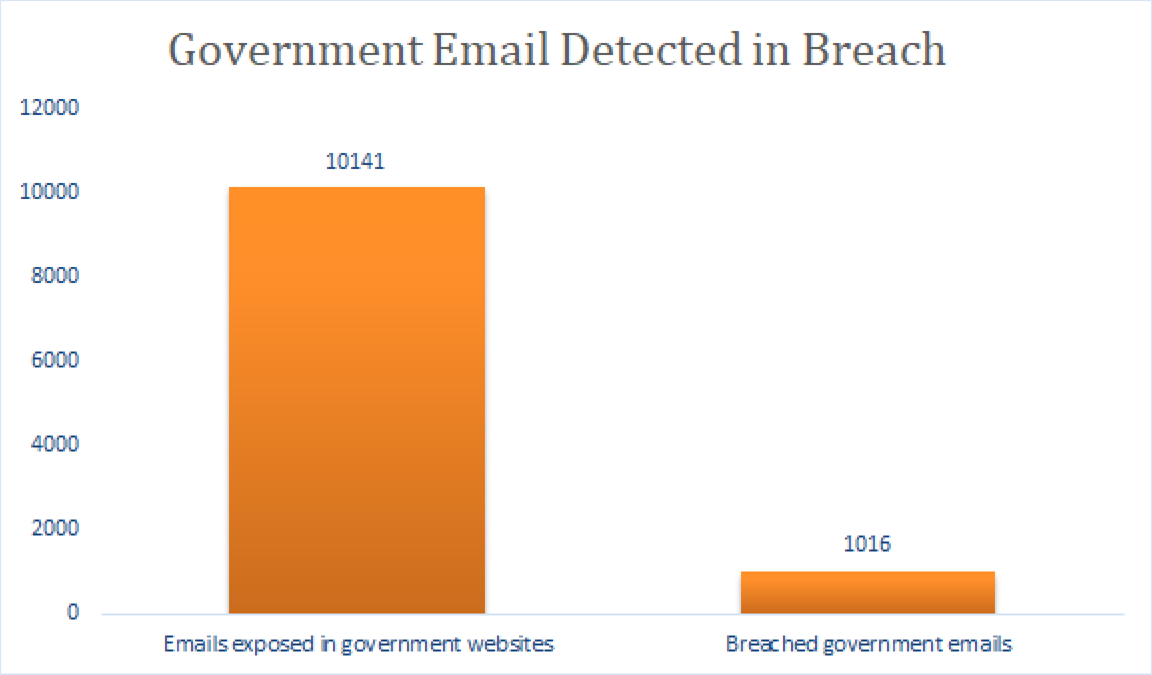


Figure 21: Government Emails in Data Breach

CVEs as indexed by Shodan

A 'vulnerability' is a weakness in a program that can be exploited to perform unauthorized actions. And CVE is a list of entries each containing an identification number, a description, and at least one public reference for publicly known cybersecurity vulnerabilities. Shodan, search engine for internet connected devices, lists the CVEs for the devices that it indexes. So, common vulnerability in any internet connected devices can be obtained from Shodan.

As per our analysis, we found 65,028 Nepali hosts indexed by Shodan, out of which 1359 hosts had at least one vulnerability with known CVE.

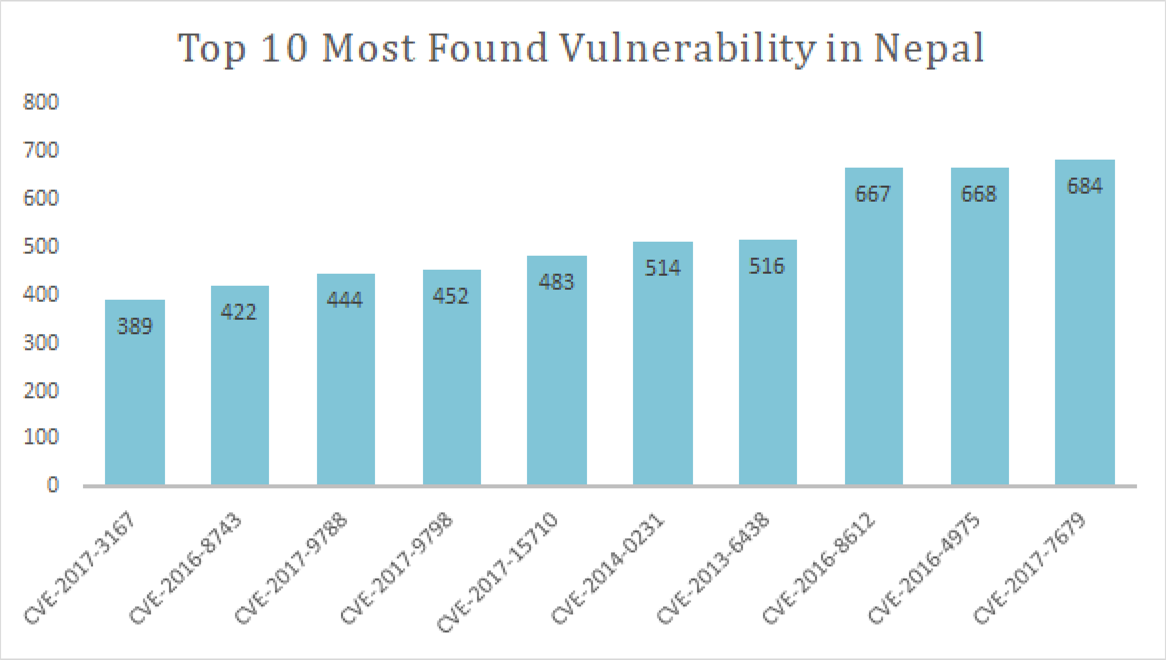


Figure 22: Top 10 most found Vulnerabilities in Nepal

WannaCry Ransomware

WannaCry Ransomware leverages CVE-2017-0144, a vulnerability in Microsoft Server Message Block 1.0 (SMBv1), to infect computers. The security flaw was exploited using an exploit leaked by the Shadow Brokers group named “EternalBlue”. The Wannacry Ransomware was a cyber-attack outbreak that started on May 12 targeting machines running the Microsoft Windows operating systems. The hard-drive encrypting malware spread rapidly because the group behind it had combined normal malware with EternalBlue, a leaked NSA hacking tool which allowed WannaCry to use worm-like capabilities to self-propagate on vulnerable Windows systems. It attempts to exploit vulnerabilities in the Windows SMBv1 server to remotely compromise systems, encrypt files, and spread to other hosts.

Even after a year of disclosure of this vulnerability, we found out 453 smb enabled devices from search engine for internet connected devices like shodan, censys and zoomeye. Out of which 7 devices were vulnerable to WannaCry Ransomware.

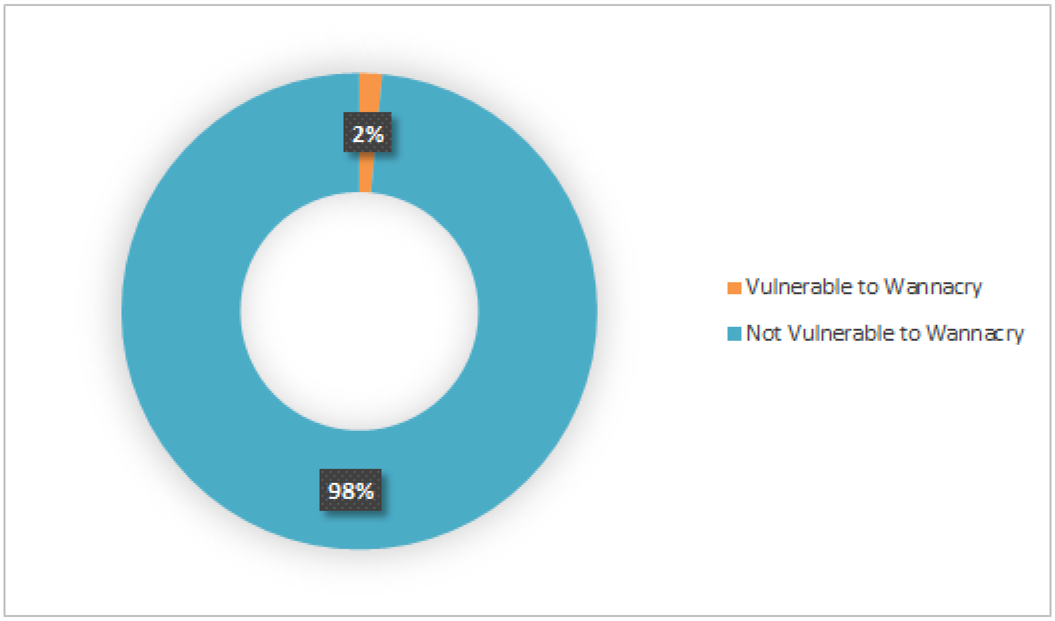


Figure 23: SMB Enabled Devices in Nepal

Comparison with Last Years' Findings

In 2017, we found out 82 SMB enabled devices and 4 of them were vulnerable to WannaCry. Although Microsoft had already released patches to address the vulnerability in March 2017 soon after the disclosure of the vulnerability, our latest findings suggests most of the organizations still have not applied these patches. Despite the damage done by WannaCry last year, the increase in number of SMB enabled devices and devices vulnerable to WannaCry this year can be attributed to sheer negligence of the respective organization.

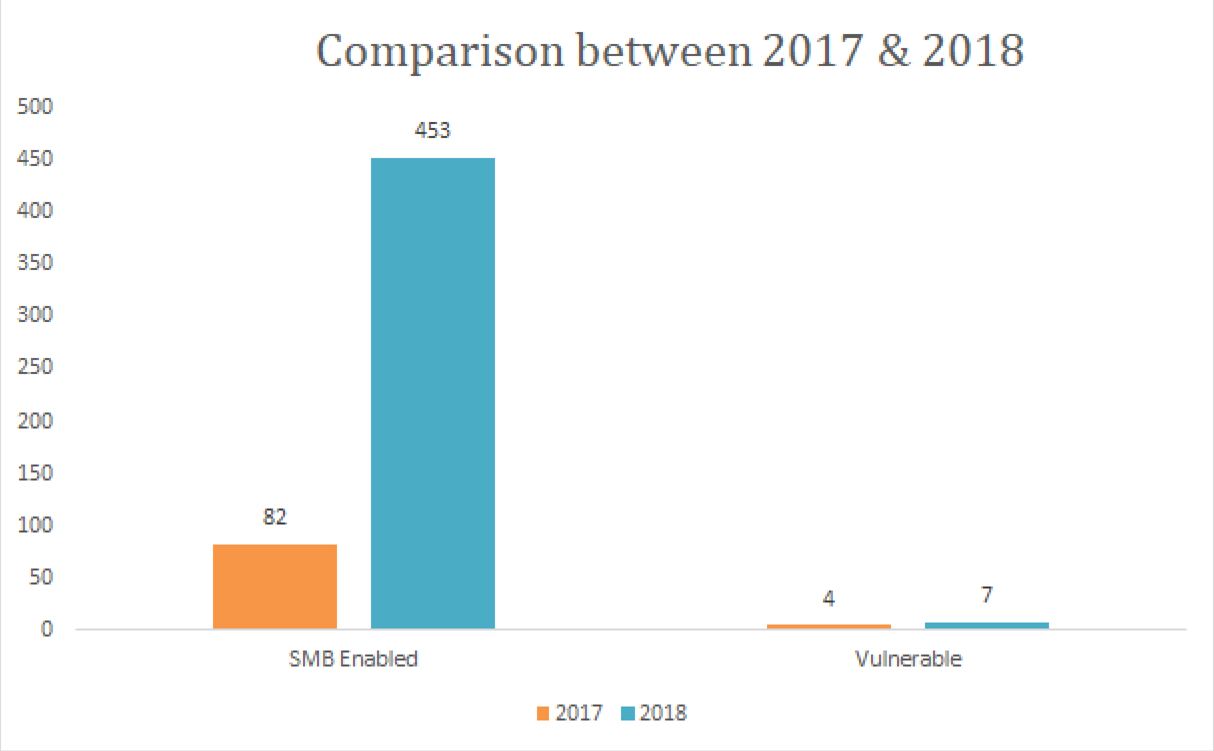


Figure 24: Comparison of WannaCry Vulnerable Devices between 2017 and 2018

Solution

To prevent your devices from WannaCry infection, ensure that all of the latest patches are applied to the systems, especially the ones related to MS17-010.

Heartbleed

Heartbleed (CVE-2014-0160), disclosed in April 2014, is a serious vulnerability that allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. This compromises the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. If the servers on your SSL environment use OpenSSL version 1.0.1 through 1.0.1f with the Heartbleed extensions enabled, then your environment is vulnerable to Heartbleed.

Although the patches were made publicly available as soon as the vulnerability was disclosed, we found 30 hosts that are still vulnerable to Heartbleed, in Nepal. These hosts belong to various organizations ranging from ISPs' infrastructure to government websites. The vulnerable hosts are categorized based on the organizations in the figure below.

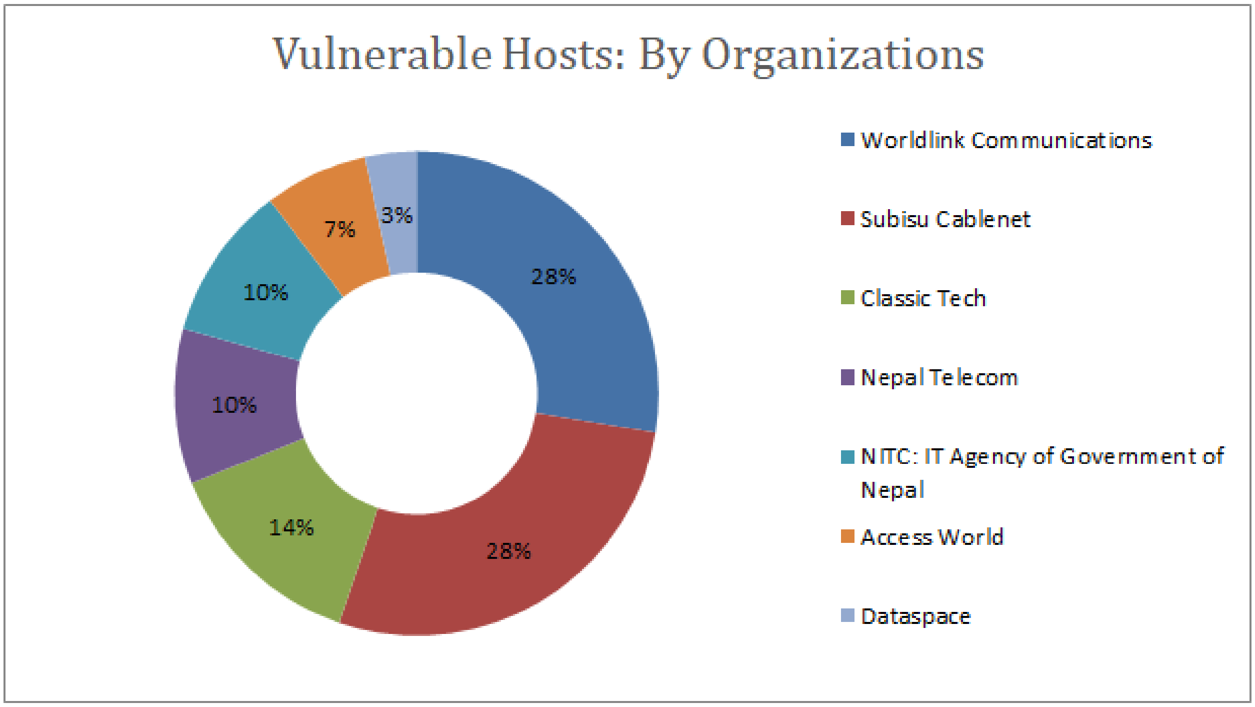


Figure 25: Hosts Vulnerable to Heartbleed: By Organizations

Comparison with Last Year's Findings

In our previous threat report for 2017, we had found 25 hosts vulnerable to heartbleed. With an old vulnerability like heartbleed, we were expecting the number of vulnerable hosts to decrease as the vulnerability is already remediated in the later releases of the product. But contrary to our expectations, we have seen an increase in the number of such hosts.

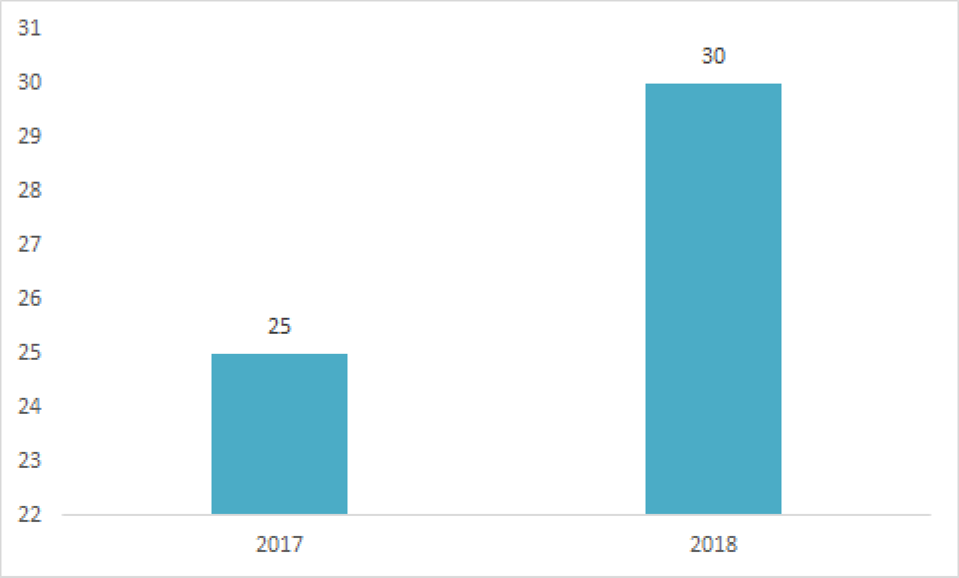


Figure 26: Comparison of Heartbleed Vulnerable Devices in 2017 and 2018

Solution

The vulnerable hosts should upgrade their servers to use the latest version of OpenSSL (version 1.0.1g or later) and rekey, reissue and then revoke all certificates used with the vulnerable version of OpenSSL.

Conclusion

Cyber Security attacks are growing, both in their prevalence and in their disruptive potential. While cyber threats are on the increase, the problem is exacerbated by the continued negligence of government and private sector. As the pace of change accelerates, and cyber security attacks intensify, we need to put more focus on strengthening our cyberspace, building defensive capabilities and identification of the potential risk to the infrastructure.

We once again stress the need for public-private collaboration on making the internet a safer place. In its place, the government and authority bodies should draft policies that mandates security standards making user data more secure and both the governmental and private entities on working together to ascertain secure handling, transport and storage of user data.

Recommendations for securing hosts and devices:

The following are the go-to steps that should be done as soon as a new host or service is set up:

- Change the default password and use strong passwords
- Setup authentication for hosts with sensitive data
- Patch the system and keep it up-to-date
- Periodic security testing of applications and hosts
- Limit access of hosts and services within required areas

We recommend developers to keep the following things in mind:

- Understand security implications and proper security implementations of a technology before implementing it
- Implement basic security practices in all places possible
- Use the principle of least privilege when it comes to access control
- Never trust data coming from a client
- Ensure that any sensitive data is not publicly accessible
- Remove all backups and restrict access to any kind of configuration files before making a website publicly accessible.

While there is much that developers and administrators can do to ascertain security of computer system, the end users still have to do their part to ensure that all the security measures are not rendered useless. End users must do the following to be safe and secure:

- Use anti-virus programs
- Use ad-blockers from trusted vendors (like NoScript for Firefox)
- Do not trust attachments received in emails
- Do not download/install/execute programs from unknown vendors and/or sites
- Turn on automatic updates for programs in use
- Use strong passwords
- Use 2 Factor Authentication, it adds a safety layer to account.
- Do not login to your accounts using public computers and free WiFi Hotspots.
- Regularly check if you have been affected in any breach by checking services like haveibeenpwned
- Never reuse passwords in multiple sites

Appendix

[1] https://www.weforum.org/reports/the-global-risks-report-2018

[2] https://badpackets.net/200000-mikrotik-routers-worldwide-have-been-compromised-to-inject-cryptojacking-malware/

[3] https://threatnix.io/2017

[4] https://web.archive.org/web/20181022094122/https://www.cvedetails.com/vulnerability-list/vendor_id-74/product_id-128/PHP-PHP.html

[5] https://www.beyondsecurity.com/scan_pentest_network_vulnerabilities_php_running_version_prior_5_3_26