



Tonga - **TCC** Security Perspective from Smaller ISP

Name : Maile Halatuituia
TCC , Network Engineer (Core Network)



Acknowledgement

1. Abstract Approval/Accept by FIRST PC
2. TCC Management Approval
3. Fellow attendance From Tonga



Introduction about myself

1. Maile Halatuituia
2. Btech in Electrical Electronic
2. Field Experienced in Internet Technology
3. Since 2001 at TCC ISP (~21 yrs.)
4. Network Engineers
5. Exposed to Linux Distributions and Window Server Env
6. Cybersecurity
7. Attend Internet/Cybersecurity Related Courses, Workshops and some Conferences too
8. I was hoping to come in person to Vanuatu for the first time but things not turn in our favor 😊
9. And here am I present Remote, thanks to technology.
10. I do hope you enjoy listening.



Name : Maile Halatuituia

TCC , Network Engineer (Core Network)



What I will talk about

Submitted Abstract

Tonga - **TCC** Security Perspective from
Smaller ISP/Operator/Enterprise



Points to Discuss

1. TCC - My Employer
2. TCC - Security Perspective
3. TCC - Statistics

Name : Maile Halatuituia

TCC , Network Engineer (Core Network)



TCC – My Employer



Background

- ❖ Began its life as “Post & Telegraph Departments”
- ❖ Later on its become Telecommunication & Telegraph Departments before late 70’s
- ❖ In late 1978 TTD split to Domestic Business named TTC (Tonga Telecommunication Commissions)
- ❖ International Business taken over by Cable & Wireless a British Telecom Company
- ❖ Early 2001 Cable & Wireless and TTC merge to form TCC
- ❖ I join TCC later the same year.

Name : Maile Halatuituia

TCC , Network Engineer (Core Network)



TCC – My Employer

Business Service for Public

- ❖ 2g,3g both Voice and Data plus LTE Data Only in our Cellular Network
- ❖ PSTN Voice Services over cables (Copper/Fiber)
- ❖ Fixed Broadband Internet Service - DSL, ADSL2+ and FTTH
- ❖ Transit Service and International Lease Circuit
- ❖ Online Customer Platform
- ❖ Limited Hosting Platform
- ❖ Main Island & Remote Islands too.
- ❖ Offer Infrastructure or Platform for e-Government Services both in Main & Remote Island



Name : Maile Halatuituia

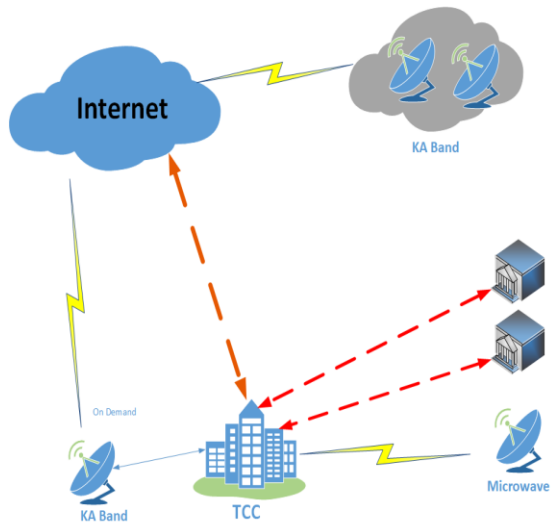
TCC , Network Engineer (Core Network)



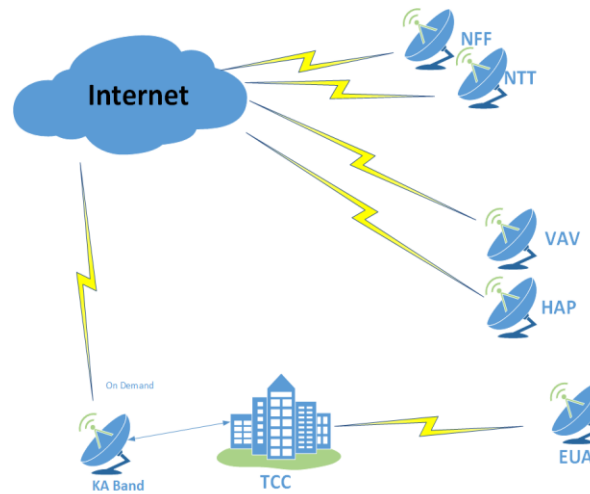
TCC – Topology

Effect of hthh volcanic Eruptions

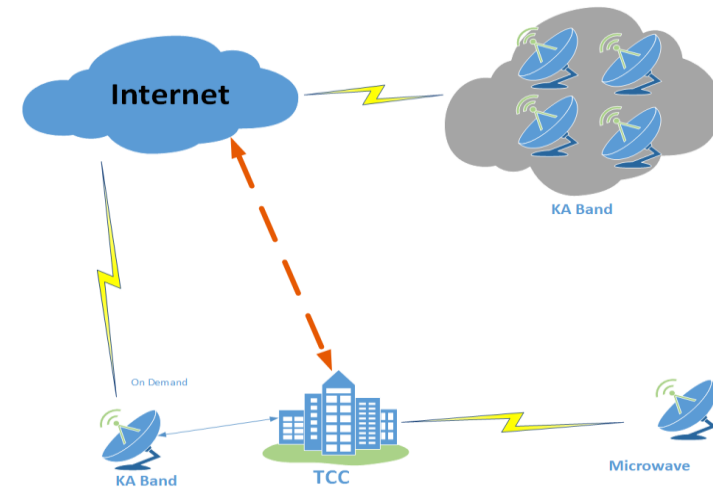
2023
FIRST
Regional
Symposium
for the Pacific
Port Vila, Vanuatu
Sep 20-22, 2023



Normal topology



- Dec 2020
- Jan 15th 2021, 3 - 4 days resume comm
- Kacific, Starlink, APNIC Router, C-Band



- Oct 2022 Int'l Cable Restored
- 12th July 2023 Domestic Restored

Name : Maile Halatuituia
TCC , Network Engineer (Core Network)



Tonga – TCC Security



- ❖ We are one of 3 Operator's in Tonga
- ❖ ~150 k Population and ~60-70% Reside in the islands
- ❖ Estimations based on this figure (Customer Based ~70k)
- ❖ Fair number of Population has Service from TCC

Name : Maile Halatuituia

TCC , Network Engineer (Core Network)



TCC – Security Perspective

Business Profile

- Telecom – Cellular and Cable Service
 - Copper and Fiber Cable Network
 - Evolved Packet Core
 - Fixed Access Network
- ISP – Internet Service Provider
 - Pre/Post Broadband Subscriber
 - Email Provider Customer/Corporate
 - NAS for Billing
 - International Carrier, Provider, Partner, Customer
 - Communication to Remote Islands
- Corporate/Enterprise – Internal TCC Business Profile
 - Corporate Services (Email, DC, Web Self-care, CDR Processing, Integration)
 - Integration's to Platforms for Billing.
 - Web Selfcare
 - Human Resource



Name : Maile Halatuituia

TCC , Network Engineer (Core Network)



TCC – Security Perspective



Few Security Challenges

- Telecom – Cellular and Cable Service
 - Mobile Core – Concern about the CIA of End User Voice & Data Access
 - The whole Infrastructure
 - Fixed Access Network – L2 Attacks , Traditional Protocols
- ISP – Internet Service Provider
 - Linux Systems Security – DNS Infrastructure
Email Services/Gateways, Subscriber Access
 - Network Security – Malware and Threat Detections, P-T-P Links
 - National and International Offices , Providers , Stakeholders , Customers.
- Corporate/Enterprise – Internal TCC Business Profile
 - Corporate Services Security
 - Secure Billing Systems Infrastructure Itself
 - Secure the Process of handling Customer Information's
 - Consider the Integrity of the Subscriber Data for Billing

Name : Maile Halatuituia

TCC , Network Engineer (Core Network)



TCC – Security Perspective

How we Deal with these Challenges



- Telecom – Cellular and Cable Service
 - User Traffic Voice and Data – 3GPP Standard Security Implementation.
 - Fixed Network Security – Protocol like Spanning tree, Block Rogue DHCP Server
 - Detect Loops on MSAN's and switches Uplinks.
- ISP – Internet Service Provider
 - Linux Systems Security – Hardening Systems (Greylists, RPZ on DNS, SPF Lookup)
 - Sadly we have not done DNSSEC ☹️ ... Live with it for now.
 - Network Security – Routing Security at the Border
 - Apply IP Base Filtering across the Board
 - Web Application Firewall and Threat Detection
- Corporate/Enterprise – Internal TCC Business Profile
 - Rely on Domain Controller (Credentials, Policy)
 - Zero Trust Approach on Network Security
 - Deploy Smart Host for Email Systems.
 - End Point Security (Defender's and Third Party) and **Threat Intelligent Tools**
 - Cloud Based Threat Detection Tools
 - Malware Detection and Threat Detections in Application Layer
 - **Deal with Human Resource (Equally Important if not more important)**

Name : Maile Halatu'ituia

TCC , Network Engineer (Core Network)



TCC – Security Perspective

Do we need to do More ? Not Restrict to TCC but in General Maybe

- Telecom – Cellular and Cable Service
- ISP – Internet Service Provider
- Corporate/Enterprise – Internal TCC Business Profile

Human Resource – Possible Weakest Links in our Cyber Security Chain.

- End User on Cellular or Fixed Service
- User in Corporate Offices, Employee on any type of Organizations
- Engineers in ISP Environment, or IT Administrators
- Security Awareness or Not
- We are all in the same category as End User of Systems
- And we will always be that Weakest Links
- Its important take extra effort to address Human
- CERT Tonga and Partners done a great Job for their Awareness Program.
- But I think there's a lot more to do



Name : Maile Halatuituia

TCC , Network Engineer (Core Network)



TCC – Security Perspective

What it is then ?



- ❖ Technological Point of View
 - Narrow the Gate – Start at the Gate and move Downstream
 - We should Inspect at the Gate and Decide what to pass and not.

Please note I don't mean **Law/Unlawful Interception**. Rather I mean there are unsecure Protocol still use today. And sadly most of Major Attack amount to these Protocols, RDP used by **Meduza** Ransomware or Samba TCP port 445 were used by other well known Malware like **WannaCry**

Blocking these Traditional Port means Hackers will work a bit more to find their Target.

- Zero Trust Approach – Never Trust, Always Verify (Borrow from APNIC) Websites
 - Home Users , Office Users , End Users , Administrators , Engineers
 - Any approach we make regarding Security whether in Office
 - At Home or in any Environment.
 - We should stop Everything/Everyone at the Gate and only Allow what is needed



TCC – Security Perspective



What it is then ?

❖ Technological Point of View

- More Cloud Based and Digitalized of Working Environment
 - Means Perimeter for Traditional Network is more Blurred than Ever.
 - Threats are Evolved and Attackers take advantage of the new Surface Appear
 - Signature Based Detection Technology help us Alert of possible Incidents
 - Still Intense Cyber Security Monitoring is Required
 - In order to detect more Sophisticated Threats that Evades Controls in Place
 - Of course this requires Resource which most of us at this end do
 - Not Have





TCC – Security Perspective



❖ Human Resource Point of View

- Train the End Users – We should not stop do that.
- Train the Trainers, Administrators, Engineers – All Human is Users of some Systems

❖ Engineers no different to End Users of our Service or Systems

- We should be equally train if not more than our End Users
- Cybersecurity Specialist Skills
- Intelligent-led Risk Assessments Skills
- Forensic Analysis Skills
- Different Level of Threats require different level of Skills

Name : Maile Halatuituia

TCC , Network Engineer (Core Network)



TCC – Security Perspective



❖ Human Resource Point of View

- From Attackers Point of View , We are all the Low Hanging Fruit
- I guess we all know **Social Engineering** is for Human not Machine or Bot
- We are the most Vulnerable Entity in Cybersecurity Chain.
- From Risky Online Behavior
- Using Insecure Password
- Irresponsible Use of Sensitive Information
- Or our Behavior on Online Platform
- These can all lead us to Exposed Secure System and ourselves to the Attackers.

A misconception at times that “Security through Obscurity”

Small , Medium and Large Organization or Users , no one is Immune to Cyberattacks

So it is important to train Users of System regardless of type we are bound to.

Now we can see some Sample Statistics we see on this end as an ISP

Name : Maile Halatuituia

TCC , Network Engineer (Core Network)



TCC – Statistics



We are the Source – Intentional/Unintentional

- Noticed of Claimed Infringement
- LeakIX Guardian
- Bit Ninja Server Report Abuse
 - Source of Abuse
- Online Database Listed like EGP Abuse
 - Our IP's being used as source of scans , probably Malware affect these End Users
- Or more direct message like this

Hello,

We have discovered a malicious web shell being hosted on your network:

hxxps://[redacted].com/aspnet_client/support.aspx [redacted] hxxps://[redacted].com/aspnet_client/support.aspx [redacted]



Loginattempts from Your net

AO ~~abuse-out@sgouros.de~~
To internet@tcc.to

We removed extra line breaks from this message.

The address ~~202.134.21.29~~ from Your network tried to log in to our network using Port 23/tcp. This is a matter of concern for us and continued tries might result in legal action. If the machin The times included are in Central European Time (CET).

Date	Sourceip	port	destips
14.07.2023 03:48:43	202.134.21.29	23	154.14.98.28

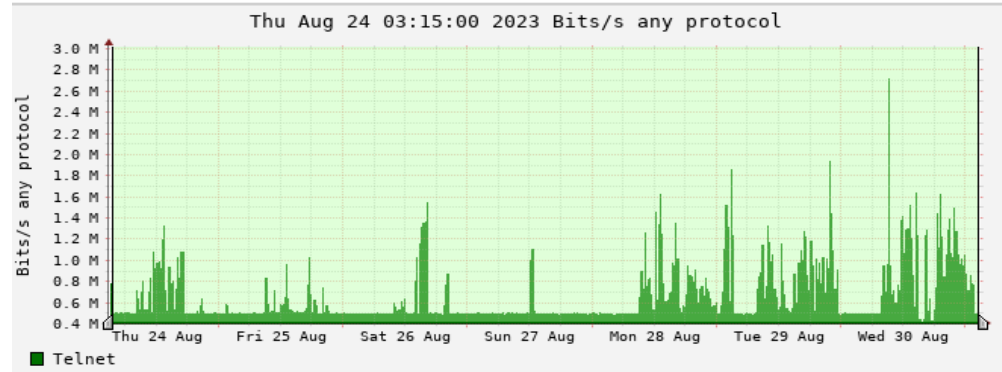
❖ In addition to this we can see few Sample Flow for Telnet, Samba and RDP in the next few slides



TCC – Statistics



Flow Data - Telnet



Netflow Processing

Source: FTP HTTP Telnet All Sources

Filter:

Options: List Flows Stat TopN

Top:

Stat: order by:

Limit: Packets

Output: / IPv6 long

```
** nfdump -M /var/nfsen/profiles-data/Telnet/Telnet -T -R 2023/08/24/nfcapd.202308240315:2023/08/31/nfcapd.202308310205 -n 10 -s ip/flows
```

```
nfdump filter:
```

```
any
```

```
Top 10 IP Addr ordered by flows:
```

Date first seen	Duration	Proto	IP Addr	Flows(%)	Packets(%)	Bytes(%)	pps	bps	bpp
2023-08-24 03:14:45.632	597995.751	any	[REDACTED]	2.4 M(38.5)	241.4 M(37.1)	14.4 G(28.7)	403	192948	59
2023-08-24 04:35:12.958	584744.509	any	[REDACTED]	844126(13.5)	84.7 M(13.0)	5.1 G(10.1)	144	69168	59
2023-08-24 16:58:45.773	531462.652	any	[REDACTED]	765289(12.3)	76.8 M(11.8)	4.6 G(9.1)	144	68993	59
2023-08-24 03:14:45.462	577970.114	any	[REDACTED]	602238(9.7)	60.5 M(9.3)	3.6 G(7.2)	104	49935	59
2023-08-24 03:53:17.333	585524.144	any	[REDACTED]	590910(9.5)	59.3 M(9.1)	3.6 G(7.1)	101	48542	59
2023-08-24 03:28:42.399	600061.707	any	[REDACTED]	334150(5.4)	34.8 M(5.4)	3.3 G(6.5)	58	43747	94
2023-08-24 03:32:00.761	599861.095	any	[REDACTED]	296813(4.8)	29.8 M(4.6)	1.8 G(3.5)	49	23694	59
2023-08-24 03:39:10.589	599433.697	any	[REDACTED]	142308(2.3)	14.3 M(2.2)	853.0 M(1.7)	23	11383	59
2023-08-24 03:26:37.420	598946.115	any	[REDACTED]	39191(0.6)	3.9 M(0.6)	234.7 M(0.5)	6	3134	59
2023-08-24 04:57:31.289	594433.653	any	[REDACTED]	5803(0.1)	7.4 M(1.1)	5.2 G(10.4)	12	70109	705

```
Summary: total flows: 6239513, total bytes: 50.2 G, total packets: 650.5 M, avg bps: 668739, avg pps: 1082, avg bpp: 77
```

```
Time window: 2023-08-24 03:14:45 - 2023-08-31 02:09:44
```

```
Total flows processed: 6239513, Blocks skipped: 0, Bytes read: 399593516
```

```
Sys: 3.881s flows/second: 1607315.8 Wall: 3.865s flows/second: 1614230.6
```

Name : Maile Halatuituia

TCC , Network Engineer (Core Network)





TCC – Statistics



Flow Data - Telnet

Date first seen	Duration	Src IP Addr	Src Pt	Dst IP Addr	Dst Pt	Packets	Bytes	bps	Bpp	Flows
2023-08-24 03:14:45.632	0.000	[REDACTED]	49176	34.183.89.141	23	100	6000	0	60	1
2023-08-24 03:14:45.667	0.000	[REDACTED]	42092	101.97.183.160	23	100	6000	0	60	1
2023-08-24 03:14:45.757	0.000	[REDACTED]	38849	94.137.174.235	23	100	6000	0	60	1
2023-08-24 03:14:46.806	0.000	[REDACTED]	52649	16.151.67.222	23	100	6000	0	60	1
2023-08-24 03:14:46.813	0.000	[REDACTED]	40862	134.121.188.29	23	100	6000	0	60	1
2023-08-24 03:14:46.847	0.000	[REDACTED]	50052	41.173.226.132	23	100	6000	0	60	1
2023-08-24 03:14:46.849	0.000	[REDACTED]	41933	156.184.62.214	23	100	6000	0	60	1
2023-08-24 03:14:47.572	0.000	[REDACTED]	51995	197.126.182.41	23	100	6000	0	60	1
2023-08-24 03:14:47.635	0.000	[REDACTED]	44590	159.43.35.11	23	100	6000	0	60	1
2023-08-24 03:14:48.007	0.000	[REDACTED]	47825	162.90.232.181	23	100	6000	0	60	1
2023-08-24 03:14:48.051	0.000	[REDACTED]	57174	195.136.155.164	23	100	6000	0	60	1
2023-08-24 03:14:48.575	0.000	[REDACTED]	33207	21.68.9.3	23	100	6000	0	60	1
2023-08-24 03:14:48.598	0.000	[REDACTED]	59511	100.253.59.104	23	100	6000	0	60	1
2023-08-24 03:14:50.377	0.000	[REDACTED]	56579	210.52.205.230	23	100	6000	0	60	1
2023-08-24 03:14:50.614	0.000	[REDACTED]	51510	113.93.78.103	23	100	6000	0	60	1
2023-08-24 03:14:50.643	0.000	[REDACTED]	43602	85.32.34.150	23	100	6000	0	60	1
2023-08-24 03:14:51.460	0.000	[REDACTED]	47900	119.39.19.48	23	100	6000	0	60	1
2023-08-24 03:14:51.497	0.000	[REDACTED]	42219	107.138.166.5	23	100	6000	0	60	1
2023-08-24 03:14:51.603	0.000	[REDACTED]	46182	112.5.253.167	23	100	6000	0	60	1
2023-08-24 03:14:51.613	0.000	[REDACTED]	53524	209.198.248.236	23	100	6000	0	60	1

Summary: total flows: 20, total bytes: 120000, total packets: 2000, avg bps: 160508, avg pps: 334, avg bpp: 60

Time window: 2023-08-24 03:14:45 - 2023-08-24 03:19:43

Total flows processed: 3089, Blocks skipped: 0, Bytes read: 197828

Sys: 0.016s flows/second: 185726.3 Wall: 0.000s flows/second: 8065274.2



Name: Maile Halatuituia

TCC, Network Engineer (Core Network)





TCC – Statistics



Flow Data – RDP Receiving End – Used by Meduza



Date first seen	Duration	Proto	Src IP Addr:Port	Dst IP Addr:Port	Out Pkt	In Pkt	Out Byte	In Byte	Flows
2023-09-14 02:01:09.258	2.271	TCP	60.240.226.218:27841 <->	[REDACTED]:3389	100	100	5200	73300	2
2023-09-14 02:00:47.107	0.000	TCP	58.171.33.27:56740 <->	[REDACTED]:3389	100	0	28500	0	1
2023-09-14 02:00:50.537	0.000	TCP	202.29.172.175:49186 <->	[REDACTED]:3389	100	0	89400	0	1
2023-09-14 02:00:18.937	0.000	TCP	202.29.172.175:53505 <->	[REDACTED]:3389	100	0	31700	0	1
2023-09-14 02:00:53.911	0.000	TCP	60.240.226.218:11583 <->	[REDACTED]:3389	100	0	33300	0	1
2023-09-14 02:00:19.513	0.000	TCP	45.227.255.4:39225 <->	[REDACTED]:3389	0	100	0	4000	1
2023-09-14 02:01:31.811	0.000	TCP	138.199.59.41:57081 <->	[REDACTED]:3389	0	100	0	71700	1
2023-09-14 02:01:19.823	0.000	TCP	139.99.250.110:49207 <->	[REDACTED]:3389	0	100	0	4000	1
2023-09-14 02:00:14.444	0.000	TCP	42.81.139.3:53211 <->	[REDACTED]:3389	0	100	0	8300	1
2023-09-14 02:00:54.146	0.000	TCP	213.136.74.180:49501 <->	[REDACTED]:3389	0	100	0	4000	1
2023-09-14 02:00:03.522	0.000	TCP	132.148.76.25:40403 <->	[REDACTED]:3389	0	100	0	4000	1
2023-09-14 02:00:45.868	0.000	TCP	58.171.33.27:56741 <->	[REDACTED]:3389	0	100	0	8300	1
2023-09-14 02:00:06.388	0.000	TCP	89.39.104.164:52629 <->	[REDACTED]:3389	100	0	9900	0	1
2023-09-14 02:01:25.263	0.000	TCP	103.228.74.153:46443 <->	[REDACTED]:3389	0	100	0	4000	1
2023-09-14 02:01:09.992	0.000	TCP	60.240.226.218:27833 <->	[REDACTED]:3389	100	0	121300	0	1
2023-09-14 02:00:21.470	0.000	TCP	138.199.59.41:49560 <->	[REDACTED]:3389	100	0	4000	0	1
2023-09-14 02:00:57.550	0.000	TCP	45.227.255.4:6473 <->	[REDACTED]:3389	0	100	0	4000	1
2023-09-14 02:00:11.013	0.000	TCP	132.148.76.25:40403 <->	[REDACTED]:3389	0	100	0	4000	1
2023-09-14 02:00:34.713	0.000	TCP	45.227.255.4:16585 <->	[REDACTED]:3389	0	100	0	25400	1

Summary: total flows: 20, total bytes: 538300, total packets: 2000, avg bps: 48776, avg pps: 22, avg bpp: 269

Time window: 2023-09-14 02:00:03 - 2023-09-14 02:04:42

Total flows processed: 63, Blocks skipped: 0, Bytes read: 4164

Sys: 0.016s flows/second: 3891.8 Wall: 0.000s flows/second: 253012.0

Name : Maile Halatuituia

TCC , Network Engineer (Core Network)





TCC – Statistics



Flow Data – RDP Receiving End



Community Score

⚠️ 5 security vendors flagged this IP address as malicious

58.171.33.27 (58.160.0.0/12)
AS 1221 (Telstra Corporation Ltd)

Similar | Graph | API

AU | Last Analysis Date: 19 days ago

DETECTION | DETAILS | RELATIONS | COMMUNITY

Security vendors' analysis ⓘ Do you want to automate checks?

Antiy-AVL	⚠️ Malicious	Cluster25	⚠️ Malicious
Criminal IP	⚠️ Malicious	CyRadar	⚠️ Malicious
SOCradar	⚠️ Malicious	CrowdSec	ⓘ Not Recommended
Abusix	✅ Clean	Acronis	✅ Clean
ADMINUSLabs	✅ Clean	AlienVault	✅ Clean
alphaMountain.ai	✅ Clean	Avira	✅ Clean

Name : Maile Halatuituia
TCC , Network Engineer (Core Network)



TCC – Statistics



Flow Data – Samba Receiving End – Use by WannaCry

Date first seen	Duration	Proto	Src IP Addr:Port	Dst IP Addr:Port	Out Pkt	In Pkt	Out Byte	In Byte	Flows
2023-09-14 10:19:46.126	0.000	TCP	59.90.196.26:52791 <->	[REDACTED]:445	0	100	0	19800	1
2023-09-14 10:20:42.381	0.000	TCP	59.90.196.26:53258 <->	[REDACTED]:445	0	100	0	4000	1
2023-09-14 10:20:35.964	0.000	TCP	41.160.52.153:56400 <->	[REDACTED]:445	0	100	0	4400	1
2023-09-14 10:20:15.867	0.000	TCP	175.176.26.69:6708 <->	[REDACTED]:445	100	0	21400	0	1
2023-09-14 10:20:43.568	0.000	TCP	59.90.196.26:53272 <->	[REDACTED]:445	100	0	38700	0	1
2023-09-14 10:20:02.632	0.000	TCP	[REDACTED]:65338 <->	[REDACTED]:445	0	100	0	5200	1
2023-09-14 10:20:22.975	1.198	TCP	59.90.196.26:53107 <->	[REDACTED]:445	0	200	0	54600	1
2023-09-14 10:20:12.698	0.000	TCP	59.90.196.26:53008 <->	[REDACTED]:445	0	100	0	4000	1
2023-09-14 10:20:26.969	0.000	TCP	147.50.41.210:53874 <->	[REDACTED]:445	0	100	0	4000	1
2023-09-14 10:20:17.545	0.000	TCP	189.186.36.10:56850 <->	[REDACTED]:445	0	100	0	4400	1
2023-09-14 10:20:19.425	0.000	TCP	59.90.196.26:53080 <->	[REDACTED]:445	0	100	0	15000	1
2023-09-14 10:20:34.696	0.000	TCP	175.176.26.69:6714 <->	[REDACTED]:445	0	100	0	11300	1
2023-09-14 10:20:41.862	0.000	TCP	123.136.30.98:58757 <->	[REDACTED]:445	0	100	0	4000	1
2023-09-14 10:20:24.863	0.000	TCP	147.50.41.210:52581 <->	[REDACTED]:445	0	100	0	4000	1
2023-09-14 10:20:52.240	0.000	TCP	59.90.196.26:53359 <->	[REDACTED]:445	0	100	0	5200	1
2023-09-14 10:20:27.418	0.000	TCP	222.71.127.234:46294 <->	[REDACTED]:445	0	100	0	4000	1
2023-09-14 10:20:13.869	0.000	TCP	59.90.196.26:53030 <->	[REDACTED]:445	0	100	0	19800	1
2023-09-14 10:20:08.725	0.000	TCP	59.90.196.26:52979 <->	[REDACTED]:445	100	0	4000	0	1
2023-09-14 10:20:14.366	0.000	TCP	175.176.26.69:6707 <->	[REDACTED]:445	0	100	0	11300	1
2023-09-14 10:20:27.793	0.000	TCP	147.50.41.210:52009 <->	[REDACTED]:445	0	100	0	13700	1

Summary: total flows: 20, total bytes: 252800, total packets: 2100, avg bps: 30589, avg pps: 31, avg bpp: 120

Time window: 2023-09-14 09:50:00 - 2023-09-14 10:24:55

Total flows processed: 81081, Blocks skipped: 0, Bytes read: 5242740

Sys: 0.060s flows/second: 1330964.1 Wall: 0.107s flows/second: 753926.3



Name : Maile Halatuituia

TCC , Network Engineer (Core Network)





TCC – Security Perspective



❖ Some Final Thoughts before we see some statistics

- We should do more Awareness.
- End Users and Systems Users a like.
- More Technical Capability to be able to Monitor, Visualize and Simulate Incidents.
- **Narrow the Gate → Blocking these Unsecure like RDP, Telnet, Samba from Internet**
- **Do we have legal Right to do that as an Operator or ISP ?**
- **Maybe we can have legal entity work out some guidelines to address it ?**
- **However existing of these unsecure connections like RDP, Samba and even Telnet on the Internet**
- **Bring out the Questions , Does local organization have Policy, maybe there is Policy but not enforce**
- **Giving the legal rights to ISP's to Block these will make Attackers think more and Work Harder.**
- **Of course we have to consider tools like Honeynet and Honeypot too.**

❖ Cyberdrills

- ❖ Local within Organizations
- ❖ Across Government Ministries
- ❖ Maybe between Same Company locate in Different Economies.

❖ With this Drills we can test the Readiness not only of the Technology in place but of course the Human Involves too before any Actual Cyberattacks Happens.

Name : Maile Halatuítuía

TCC , Network Engineer (Core Network)



TCC – Security Goodbye 😊



If you have Question/Comments please send me an email
Email : maile.halatuituia@tcc.to



Thank you all for listening

Malo Aupito

Name : Maile Halatuituia
TCC , Network Engineer (Core Network)