No.56
July 2022

HardenStance Briefing

Trusted research, analysis & insight in IT & telecom security **PUBLIC/UNSPONSORED**

Threat Intel in Telecoms (TTIS2022)

On June 22nd – 23rd, HardenStance hosted the 2022 Telecom Threat Intelligence Summit (TTIS2022). This executive summary includes a link to the event recording.

- Cybersecurity leaders from Deutsche Telekom, KPN, Telus and Lumen shared threat intelligence best practice in telecoms with the TTIS 2022 audience.
- Current and former telco CISOs, as well as the UK's NCSC, chose to focus more on ongoing challenges with calls to fix a "broken" model, "regulate" to assure the visibility that excellent cyber security requires, and "demand better" from vendors.
- GSMA's new 'MOTIF' group is advancing normalization in the way mobile cyber threats are described. As well as participating in MOTIF, MITRE is targeting a first release of its new 'FiGHT' threat intel framework for 5G in the coming months.

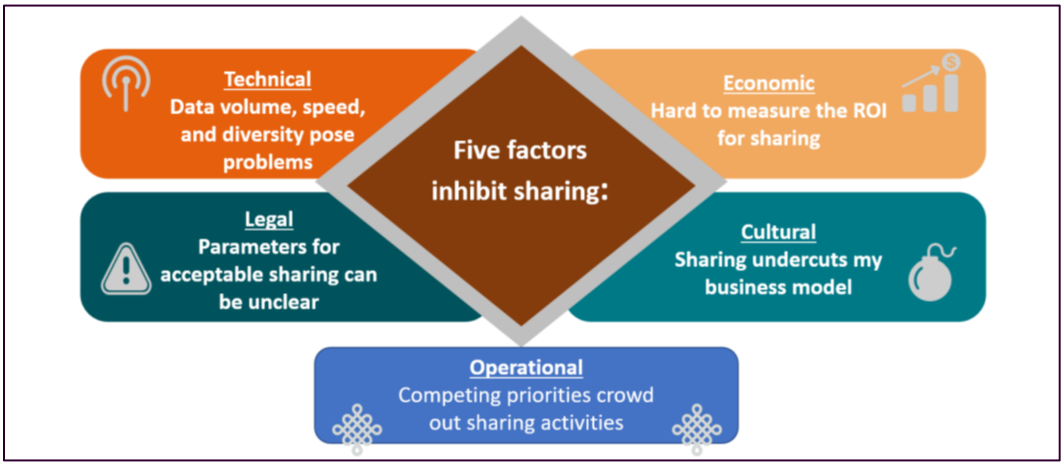
Overcoming Barriers to Threat Intel Sharing

Noting how threat intelligence sharing "never seems to quite live up to its promise", CTA's Michael Daniel provided guidance on how to frame strategic thinking around using and sharing threat intel.

Michael Daniel, President of Cyber Threat Alliance, emphasized how challenging it is to embed good use of cyber threat intelligence in an organization's cyber security and broader risk management processes. Noting how threat intel sharing "never seems to quite live up to its promise", Michael guided TTIS 2022 on how to frame strategic thinking around the use of threat intel. He stressed the importance of being clear about different types of threat intelligence – technical, tactical, operational and strategic – and the consumption of that intel by different groups within a telco or other organization. He also pointed to factors that routinely inhibit sharing, which have to be monitored and navigated around, in some cases on an ongoing basis. Specifically he pointed to:

- **Technical**: Michael said "we're actually drowning in data" in terms of the immense volume, speed and diversity of data and data formats that are out there.
- **Economic**: It's very hard to measure the ROI on threat intel sharing.
- **Legal:** There are constraints around what organizations can share such as with GDPR which considers IP addresses to be Personal Identifiable Information (PII).

Figure 1: Why Information Sharing is Hard


Technical
Data volume, speed, and diversity pose problems
Economic
Hard to measure the ROI for sharing
Five factors inhibit sharing:
Legal
Parameters for acceptable sharing can be unclear
Cultural
Sharing undercuts my business model
Operational
Competing priorities crowd out sharing activities

Source: Cyber Threat Alliance

- **Cultural:** Some organizations – or some people in some organizations – think threat intelligence sharing undermines their competitive edge because they mistakenly believe a significant part of their value comes from the amount of data they have.
- **Operational:** There are always other priorities besides threat intel sharing.

From his many years of experience, Michael concluded that high quality information sharing requires investment – of money, time, attention and trust. He also stressed the importance of driving threat intelligence strategy from a policy and process perspective rather than just focusing on buying the latest technology enabler.

KPN’s Use of Threat Intel is Relatively Advanced

Championing it as the “backbone” or “anchor” of good cyber security, KPN’s VP Security, Erno Doorenspleet, shared how the incumbent telco in the Netherlands uses threat intelligence in its security operations. He emphasized the cumulative power of threat intelligence when properly curated, interpreted and communicated to serve four distinct stakeholders. He cited the first three as IT and security analysts, the Security Operations Centre (SOC) and the Computer Emergency Response Team (CERT). Fourth, Erno pointed to consumption by executive management: “the power is in taking data that starts off as highly technical and translating that into digestible insights for executive management. They need to understand what the threat intel says and what the implications are for the business. If you do that right, they can leverage that intelligence to make the right decisions as part of their risk management portfolio.”

KPN’s Erno Doorenspleet noted uniquely challenging aspects of a telco network environment which can deny a security team some of the monitoring and logging data it needs.

Combining third party feeds with a telco’s own threat intel

As with any relatively advanced security operation, KPN Security combines third party feeds with threat intel that it generates itself, including via its own forensic investigations. KPN Security’s research team produces reports on issues as diverse as malware families and cybecrime groups. “As we all strive for automated defence, you can have the latest firewall or SIEM or SOAR platform or whatever”, Erno said, “but what’s the point without great threat intel? With the right threat intel, you can lower the number of false positives “which are what irritates the hell out of SOC people. Then you can get to a higher level of automation and your response times improve.” He also noted uniquely challenging aspects of a telco network environment, which can deny a security team some of the monitoring and logging data it needs. He cited “some components which don’t integrate properly with standard security solutions. We then have to build our own solutions to get the data out that we need and also get the threat intel in there to lower the risk.”

Erno concluded by stating: “we underestimate the power of collaboration. If we want to beat the opponent, we need to share. If we don’t, then basically they win. Sometimes it is challenging to share. But when you do, when you are part of GSMA or ETIS for example, you share knowledge and influence the way we all go forward, we can make a difference. Our mission is to break the traditional barriers to sharing.‟

Deutsche Telekom’s Threat Intel Choices and Challenges

Combining externally sourced and internally generated threat intelligence was also a core theme of the talk by Manuel Kamp, Deutsche Telekom’s Head of Threat Intelligence. In terms of the internally generated components, Manuel pointed to DNS and Netflow data as well as honeypots (which it uses to engage or interact with attacker and learn of new threats) and black hole monitoring (for passive monitoring of unused IPv4 and IPv6 addresses and detect botnet scanning).

Layered Threat Intelligence to Defend Consumers and SMEs

Angel Fernandez, AVP Security Solutions for Allot, spoke to the use of threat intelligence by telecom operators enhancing security for consumers and Small and Medium Enterprises (SMEs). His talk focused on how traditional threat intelligence databases continue to have value in protecting these customer segments but that they are becoming commoditized. He argued that they must be augmented with best practice layered and orchestrated security. That includes how to respond to threat intelligence that comes in as well as enhanced detection capabilities driven by Machine Learning and AI.

Angel described a good threat intelligence database as one that aggregates, consolidates and integrates multiple factors like signatures, IPs, domains, heuristics, and third party feeds generated both internally by a vendor and its customers as well as by third party partners. Ensuring that this is constantly updated provides a basic view of current malicious activity on the Internet which is an important foundation. Allot augments this with a layer of supervision and validation around the actions implied by what comes into the threat intelligence database. Rather than automatically acting on all intelligence – rather than automatically implementing every potential block, for example – Allot proactively verifies likely network impacts against metrics such as the volume of traffic that is going to be impacted. This allows a risk-based judgement to be made around how to respond. As Angel explained: "How to implement the threat intelligence is just as important as the quality of the threat intelligence itself."

The first example he gave of applying ML and AI to threat intelligence was for the detection of Domain Generation Algorithms (DGAs). These are used by some malware families to generate domain names which then use them to interact with their command and control servers. As these domain names are typically used for no more than a few hours there is typically no time for traditional threat intelligence databases to be updated in time to protect users. Another example is the use of Convolutional Neural Networks combined with AutoEncoder (CNN-CE) for anomaly detection once a device has become infected and is behaving in an unexpected way.

Having described the DevOps-driven architecture that underpins Deutsche Telekom's approach to embedding threat intelligence in its cyber security posture, Manuel pointed to four challenges its model either has presented or continues to present:

1 **It takes time to fully understand the content of different data sources**: understanding how to detect malicious behaviour from a large enough amount of data and then introducing a program to respond effectively can take several months.

2 **Large amounts of data are not always easy to handle:** as an example, DT's DNS servers are currently generating 2.5 Terrabytes of data every day. To support that, DT has undertaken an extensive evaluation of the most efficient solution for storing that amount of data.

3 **Automation and machine learning helps.** If a task occurs more than once, steps should be taken to automate it, including by leveraging machine learning.

4 **Data privacy requirements must be baked in.** Regulations must be complied with which imposes some constraints on security policies.

Manuel concluded by saying that "there is not one architecture" for leveraging threat intel. Data sources come in different formats and volumes. There are varying requirements from different stakeholders – management, data scientists, the SOC and CERT teams – and different subsequent uses of data beyond initial target stakeholder groups. He recommended mapping different choices to different data sources.

Ex Telco CISO Says Threat Intelligence Model is 'Broken'

Jaya Baloo, formerly with Verizon, France Telecom and KPN, now Avast's CISO, chose to challenge the TTIS audience with a talk predicated on the notion that, actually, the threat intelligence model in telecoms is "broken" and should be more use case focused.

Jaya acknowledged there are areas where more threat intel sharing is required based on relationships between telcos that already exist. She cited Border Gateway Protocol (BGP) as one example, saying "it's amazing how much political activity you can uncover from monitoring it." It's an area "where we need more data" to enable us to arrive at "a single, holistic solution to being able to view what's going on." Jaya also said there is more that telcos can do to work with peering parties to get at the origin of DDoS attacks.

Much of the rest of Jaya's talk focused on pointing out the limitations and failings in how the telecom sector can sometimes engage in too much threat intel sharing or even fail to act on known threats that pose significant risk. We're flooded with threat intel, we lack enough context, there are still far too many false positives, she said – "we need to focus on what's relevant to me, to my organization, no more generic crap." Sometimes in the telecom sector, she said, people share too much with too many people across too many meetings. "We don't always share the right information quickly enough to be able to enrich it. We have to be "a bit more choosey" about who we share with, do a better job of "finding the right friends" and focus on satisfying more specific use cases.

If we are giving people SS7 links to then subsequently perpetrate abuse, we should deny them access to the network.

Jaya concluded with a number of recommendations, of which the following are a subset:

- Truly understand the assets we have and how important they are "before we do any of the fancy threat intelligence stuff." That means assets - "because, no offence, we still suck at that" – it means threat and vulnerability management, and it means our Internet footprint.
- Share and enrich information in an automated and consistent fashion to arrive at a trusted community without having to go to 40 meetings – "and don't lurk in the background. If you just want to sip from the straw without contributing anything yourself, that's not going to work long term."
- Get better at defending forward: "If we are giving people SS7 links to then subsequently perpetrate abuse, we should deny them access to the network. Also, if we are allowing our peering parties to give us spoofed traffic, they should no longer be our peers."

Telecom-Savvy Attackers and Tech Giants Pose Challenges

Orange Polska's CISO, Przemyslaw Deba, outlined the unique mix of information assets available to a telco in support of its cyber security goals. He cited DNS (for redirecting malicious traffic); Netflow (for tracking connections); convergence (in terms of access to data from IP addresses to mobile network information and from messaging to telephony) BGP sinkholes (for separating out malicious traffic) and network visibility.

He shared that on any given day, his security team typically sees millions of DNS requests; a million domains never seen before; 20 million new certificates, of which a million appear for the very first time. The team typically has to extract 500 new phishing domains every day. ML-driven automation is progressing here. Przemyslaw specified that in terms of the way domains are qualified, the current ratio between qualifications that are fully automated and those requiring final manual confirmation is about 50/50.

He pointed to the cyber security challenges posed by telecom-savvy threat actors and by the modus operandi of tech giants or webscale companies. He chose the recent Flubot SMS and MMS-borne Android malware as an example of the former. This was able to steal passwords, online banking information and other sensitive data from infected smartphones all over the world over a period of several months (see also David Rogers comments for GSMA on page 7). Przemyslaw described Flubot as "the first of its kind to be so painful for telecoms" because it generated millions of messages from customer accounts, a large proportion of which were international. Flubot was expressly designed to be invisible to telcos. Multiple techniques – Domain Generation Algorithims (DGAs) to create domain names, encrypted communications to C2, DNS over HTTPS, changes in the message schemas to avoid detection - were used to obfuscate it. Having been taken down by law enforcement authorities, Flubot was not currently functioning at the tiem of TTIS2022 but Przemyslaw predicted that "it will certainly revive in some form, given the effectiveness of the methods used."

In the case of the webscale companies, Przemyslaw depicted them as "systematically taking over the Internet and the most valuable data sources." Widespread encryption also "prevents any meaningful inspection and hinders communication with the client." Telcos are "left with a blind pipe and low value Netflow data" he said, "so, sure, telecom operators occupy a unique position in the ICT ecosystem – but for how much longer?" Przemyslaw pointed to more favourable regulations as an important part of the solution: "I am afraid that the only way to survive, to assure visibility and transparency, is some kind of laws, some regulations. I think we can count on the EU here."

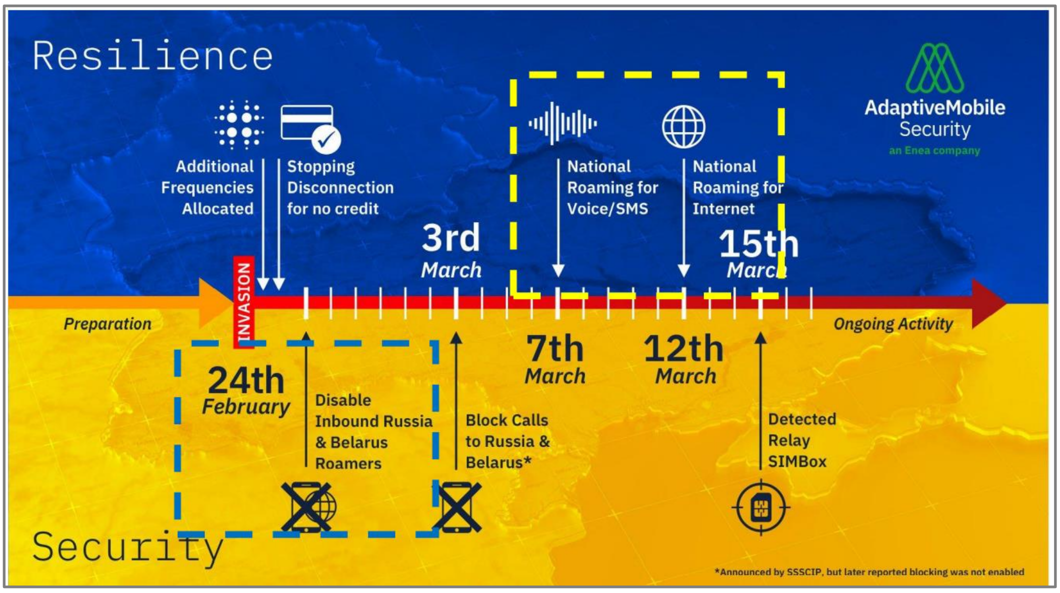
Orange Polska's CISO, Przemyslaw Deba predicted that Flubot "will certainly revive in some form, given the effectiveness of the methods used."

The Criticality of Mobile Networks: Learnings from Ukraine

Cathal Mc Daid, CTO of Enea AdaptiveMobile Security, detailed the very positive impact that a well-planned, multi-layered approach to protecting and using mobile networks has had on Ukraine's defensive war effort against Russia. He noted that Ukraine's three mobile operators have executed very well on two critical initiatives that had never previously been implemented anywhere on such a large scale. The first was to disable incoming roaming from Russian and Belarussian-registered SIMs when the invasion began. This prevented Russian forces from using Ukraine's mobile networks as they had done in previous military campaigns. The second was to enable emergency national roaming for Ukrainian subscribers to assure nationwide mobile service availability, including against physical damage in affected combat areas.

Secure and resilient mobile networks have served as a platform for the public morale-boosting effects of Ukrainians, including the national leadership, being able to post videos of their successes while denying Russian forces the same capability. The location tracking capabilities of the mobile networks have also been used in military operations including the targeting and elimination of a Russian General.

Figure 2: Ukrainian Mobile Network Responses to Russia's Invasion


Resilience
AdaptiveMobile Security
an Enea company
Additional Frequencies Allocated
Stopping Disconnection for no credit
National Roaming for Voice/SMS
National Roaming for Internet
3rd March
15th March
INVASION
Preparation
Ongoing Activity
24th February
Disable Inbound Russia & Belarus Roamers
Block Calls to Russia & Belarus*
7th March
12th March
Detected Relay SIMBox
Security
*Announced by SSSCIP, but later reported blocking was not enabled

Source: Enea AdaptiveMobile Security

Coupled with government-designed apps, the mobile networks have also been the platform for crowdsourcing operational intelligence from citizens on the ground in combat zones. Cathal reflected that Ukraine's experience to date "hasn't been the cyber war that many pundits predicted at the outset. There have been no big power outages. The cyber conflicts in this war are much more related to helping the kinetic conflicts. Therefore we can't think about cyber war on its own. We have to think more about hybrid warfare scenarios."

SS7 attacks have been attempted using captured infrastructure

Cathal also shared examples of the types of cyber threats that nation state threat actors are liable to level at mobile networks, whether that be in peacetime or during a war. He cited the Head of Ukraine's Information Security and Cyber Security Service stating recently that her department had "seen attempts to use captured telecommunications infrastructure to conduct attacks including SS7 attacks."

He also cited AdaptiveMobile's own threat research into a Russian state threat actor it labels 'Hidden Art". This carries out location tracking as well as voice and SMS interception on individuals of interest to the Russian state. When AdaptiveMobile started investigating 'Hidden Art' the purported source of the malicious messages was an African mobile operator group. Further investigation found that the purported source and the actual origin source were not the same. With its customer and multiple inter-carriers, AdaptiveMobile was able to trace the actual origin source to a Russian origin point code.

When AdaptiveMobile started investigating 'Hidden Art' the purported source of the malicious messages was an African mobile operator group.

The Latest Threat Landscape Insights from NETSCOUT & Fortinet

NETSCOUT and Fortinet each shared highlights from their threat research team's latest reports – the FortiGuard Labs Threat Report and the NETSCOUT Threat Intelligence report.

Direct Path Attacks were the Single Biggest DDoS Attack Type in 2021

Roland Dobbins, Principal Engineer, NETSCOUT, reported that at 9.7 million, the number of DDoS attacks NETSCOUT saw world-wide in 2021 was 3% down on 2020. Nevertheless, since this was still 14% up on 2019, he pointed to the opportunities presented to attackers by the disruption of the Coronavirus pandemic as having set a new floor for DDoS attack volumes. He pointed to a substantial change in the mix of DDoS attack types seen during 2021. The recent surge of reflection/amplification DDoS attacks has been abruptly halted and sent into reverse. Most strikingly, the number of Domain Name System (DNS) amplification and Connection-less Lightweight Directory Access Protocol (CLDAP) amplification DDoS attacks was down 32% and 64% year on year respectively. This left direct path attacks as the single biggest DDoS attack type in 2021. Roland pointed to the operator community's work in steering this change – especially faster adoption of anti-spoofing or source address validation solutions at customer edge sites. Roland also reported on the rise in server-class botnets.

An Exponential Acceleration in the Rate of Vulnerability Exploitation

Derek Manky, VP, Threat Intelligence, Fortinet, pointed to a new metric that Fortinet's threat research team is tracking now – the "rate of exploit". He pointed to how the recent Log4j vulnerability was fully weaponized – exploit code released - within just 24 hours. Fortinet observed no less than fifty times more Log4j-related activity at the seven-day mark compared with what it saw one week into the ProxyLogon Microsoft Exchange vulnerability less than a year earlier. "This is not a linear trend, this is exponential," Derek explained. What's driving it in the case of Log4j is that it is forming part of ten different cybercrime campaigns – different payloads ranging from Remote Access Trojans (RATs) to ransomware and crypto-miners are all exploiting the vulnerability. "From a kill chain perspective, things are happening in a super-compressed timeframe now which is very concerning," Derek added. He also highlighted how some of these types of behaviours would typically be associated with nation state threat actors, but that Fortinet is increasingly seeing them from private sector cyber gangs too now.

Cathal concluded by again advocating, as he did at the inaugural TTIS2021 last October, for a common language for expressing the activity of cyber threat actors targeting mobile networks. He pointed to progress made since October, notably the formation of MOTIF within GSMA (see page 7) which AdaptiveMobile is a member of. Cathal specified the importance of defining industry norms for sharing the Tactics, Techniques and Procedures (TTPs) of threat actors like Hidden Art. He noted that while exact source information can't be revealed relating to such threats, more effective sharing of TTPs has substantial value to telco security teams.

Mobile Network Threat Intelligence Sharing Frameworks

David Rogers, Chair of the GSMA's Fraud and Security Group (FASG), reminded TTIS2022 that adversaries are well practised at sharing intelligence amongst themselves. They've also built a lot of tooling that automates attacks and obfuscates them. He spoke of the need to be extremely agile in terms of sharing Indicators of Compromise (IoCs) and other details to help identify and understand threat actors and their behaviours. A key priority for the FASG is to enable the mobile services industry to automate threat intel sharing in structured, machine-readable, formats. David pointed to relevant telephone number ranges involved in Wangiri scams and command and control domains as data that has to be shared very quickly and that can only be done effectively in a machine readable format.

A key priority for GSMA's FASG is to enable the mobile services industry to automate threat intel sharing in structured, machine-readable formats.

David reported that a start has been made. There is a MISP-based information sharing platform up and running. In May this year the GSMA hosted the first Telecoms Information Sharing and Analysis Centre (T-ISAC) Summit. This followed the publication last November of the T-ISAC Insight report on Flubot. As of July this year, the T-ISAC will have 176 members of which 122 are mobile operators. Within FASG, a new MObile Threat Intelligence Framework (MOTIF) grouping has also been set up. This has the goal of advancing normalization in the way mobile cyber threats are described so as to enable more effective threat intel sharing across different industries and industry groupings.

MITRE's new 'FiGHT' Framework for 5G Threats

MITRE, the driver of the MITRE ATT&CK Framework, is one of the members of MOTIF. One of the goals shared by GSMA and MITRE is to converge the work they're doing in defining and sharing cyber threat intelligence as it relates to the mobile network services domain. Muddasar Ahmed, MITRE's Principal Cybersecurity Architect, and Dr Michaela Vanderveen, Principal 5G Security Architect, spoke jointly at TTIS2022, presenting MITRE's FIve G Heriarchy of Threats ('FiGHT') framework for describing, documenting and sharing 5G threats. Building on existing security frameworks, they described 'FiGHT' as a threat based framework for assessing the confidentiality, integrity and availability of 5G Networks and the systems and applications using them as well as " a model to assist with cyber investment planning and security automation for deployments."

Like the ATT&CK Framework itself, 'FiGHT' is pitched at a middling level of abstraction. Muddasar and Michaela described it as more detailed than highly abstract frameworks like the Lockheed Martin Kill Chain but also less detailed than something like Common Weakness Enumeration (CWE) or MITRE's own Common Vulnerabilities and Exposures (CVE). The MITRE speakers emphasized that, consistent with these being early days in terms of 5G roll out, FiGHT is in its formative stages with a view to making it publicly available in the coming months.

Network Based Detection and Response for the 5G Era

In the context of 5G, Nelson Silva, Security Product Manager with Nokia, discussed the emerging requirement for endpoint detection and response for mobile network security strategy - and how threat intelligence feeds into that. He pointed to the risk of simply porting the sort of agent-based endpoint detection model used in enterprise security into telecoms because of the way that can interfere with the unique network operations, service operations and service assurance requirements of a telecom network.

Nelson showed how this drives a requirement for the “security augmentation of the network” via a network-based or agentless approach to detection and response. This detects malware leveraging the Nokia Threat Intelligence Centre to analyse network traffic that’s encapsulated in tunnelling protocols like GRE, MPLS, VLAN and GTP. He pointed to this requirement between devices; between network segments; and between the internal network and the Internet. He concluded that “the focus must be on telco-specific detection requirements that are resource, service and network-aware, and telco-specific response orchestration and service assurance processes.”

Nelson from Nokia drove awareness of the shift within the DDoS threat landscape away from spoofed IP addresses driving reflection amplification attacks to more direct path attacks.

Echoing Roland from NetScout’s comments on page 6, Nelson also drove awareness of the shift within the DDoS threat landscape away from spoofed IP addresses driving reflection amplification attacks to more direct path attacks - especially those driven by botnets. This, he said, should drive adjustments in a telco’s DDoS protection strategy, notably augmenting security in the network via the operator’s router infrastructure.

How Telus Handled Threat Intel with a Major DDoS Threat

Tim Allsopp, Senior Strategy Manager for Telus, shared how earlier this year his company participated in a coordinated industry effort to minimise the major risk arising from CVE-2022-26143. This was identified in February, when a spike in DDoS traffic was seen sourced from UDP port 10074 targeting ISPs and other organizations. It was identified as arising from a vulnerability in Mitel’s MiCollab and MiVoice Business Express collaboration systems for SMB and SOHO users. It scored 9.8 on the CVE scale of 1 – 10 because it was identified as having a theoretical amplification factor of 4 billion:1. The largest comparable amplification rate Telus had previously seen was 9,000:1.

Direction from the UK’s National Cyber Security Centre (NCSC)

Peter Haigh, Director of Telecoms for the UK’s NCSC showed some empathy for the telecom sector in his talk. He said that “being a security expert in telecoms is hard because you’ve got OTT players above you removing your margin and then you’ve got regulators underneath you removing your margin. Ultimately, security is a cost so it’s not really a surprise that there’s not much of that money to go round to make sure you’re good at security.”

Peter nevertheless argued that telecoms “arguably is lagging behind other sectors”, noting some failings in telco security operations which he sees too frequently. Although recognizing some of the challenges in the telco context, he considered it “weird that we still find ourselves asking in 2022 ‘should we be patching in telecoms?’.” He also shared with dismay his estimate that no more than 50% of telco binaries are currently using Address Space Layout Randomization (ASLR), now widely adopted in enterprise security to defend against buffer overflow attacks on operating systems. Peter concluded with the following appeals to telecom operators and vendors:

The NCSC’s Guidance to operators:

- Please scan you own infrastructure from the outside.
- Your management plane is the crown jewels. Protect it.
- Please manage your third party admins properly (vendors, MSPs, SIs etc).
- Please understand what’s in your network, what’s exposed and how attack paths could materialise.
- Please demand better of your vendors.

The NCSC’s Guidance to Vendors:

- Third party and open source components are your responsibility. Sort it.
- The year 2001 called and would like its security model back. Time to get modern. API contracts, ASLR, Data Execution Prevention (DEP), fuzzing with code coverage metrics etc are your friends.
- Please build things that are securable and upgradeable.

As well as sharing some details of the investigation and response to CVE-2022-26143, Tim talked about the theme of opportunity and risk with threat intelligence sharing which Telus had to return to time and time again. Telus was initially notified of this risk by an ecosystem partner. Through each phase of the subsequent investigation and response, Telus had to repeatedly review the optimal balance between responding to protect its own network; getting the threat intelligence out to trusted defenders to help them protect their systems; and the risk that with wider dissemination of the intel, bad actors would learn of it and leverage the vulnerability to cause harm.

Tim Allsopp talked about the theme of opportunity and risk with threat intelligence sharing which Telus had to return to time and time again.

In the U.S the JCDC Has Been Built in Layers over Years

The talk on "Creating New Norms for Ecosystem Protection" by Lumen's Senior Director of National Security and Emergency Preparedness, Kathryn Condello, is a good way of concluding this report on TTIS2022. While Kathryn concluded with comments on America's new Joint Cyber Defence Collaborative (JCDC), established by the Cybersecurity and Infrastructure Security Agency (CISA) in August 2021, her talk spoke to the various layers of threat intelligence sharing that have built up in the U.S dating back to Presidential Policy Directive (PPD) #63 under President Clinton in 1998. This called for the creation of Information and Analysis Centres (ISACs) between private and public sectors, of which the Communications ISAC was one of the first. Kathryn walked attendees through various phases in the evolution of the threat intelligence collaboration model in the U.S to demonstrate what capabilities need to already be in place to allow evolution to the next level of collaborative maturity.

Concluding on the mission of the new JCDC, Kathryn described it as "coordinated operational planning and execution and collaborative cyber security fusion and analysis.‟ She specified that JCDC requires members go beyond merely sharing intelligence bilaterally. Rather, members are required to merge and aggregate their data and do further analysis on it to extract additional insights. JCDC is then charged with rapid production of defensive guidance for dissemination to broader stakeholder communities.

The Changing Responsibilities of a CISO In a Telco Organization

Omer Koker, former CISO of Vodafone Turkey, now Founder of ObjectS Consulting, pointed to the changing role of a telco CISO. He noted that CISOs increasingly have to serve as an orchestrator and aligner of people in addition to understanding what it is they're trying to defend. Using a 'mind map', Omer showed the increasing number and variety of inter-personal interfaces a CISO needs to have into legal and regulatory departments, other technical departments as well as intelligence organizations, pointing out how that 'mind map' will inevitably continue to grow.

Omer noted the growing complexity of security operations, driven by a proliferation of technologies and vendors. He speculated that outsourcing to managed service providers will become "inescapable for all but the largest organizations." By implication that could imply some, perhaps many, smaller telcos and ISPs. He also spoke to how trends in 'techno-nationalism' are increasing risk for telcos, ranging from "BGP tricks" to embedded capabilities – "three lines of code from among tens of thousands can lose you the farm." He said China has been "a major concern and I have to say from experience, not without reason." That said, he added that "from the perspective of a CISO in critical infrastructure, whether a backdoor is deliberate or not doesn't matter much - a vulnerability is a vulnerability."

He also shared his thoughts on the use of AI in cyber offence and defence: "I've seen tools under development that can collect tremendous amounts of active and passive recon information from a truly amazing number of sources in hours that would normally take weeks or months for a group of hackers to put together. More worryingly, they can do this in parallel, targeting multiple organizations. In the coming years, our bar for cyber security has to move to a higher level because AI isn't just going to be used to defend our systems – it's going to be used to attack them too.

Kathryn cited initial JCDC work relating to the Log4J vulnerability and Russia's invasion of Ukraine as "large and complex enough that JCDC as a multilateral organization is starting to build muscle memory to work on this basis." She assessed the JCDC materials published to date as "a degree above what has been done in the past". Kathryn concluded by referring to some initial engagements which the JCDC has had with international partners in the context of Russia's invasion of Ukraine. She spoke of a need to look further into the extensibility of what JCDC is doing into other domains, describing that as "work to be done." ■

View the TTIS2022 Event Recording

TTIS2022 was sponsored by AdaptiveMobile Security, Allot Ltd, Nokia, NETSCOUT, and Fortinet as well as co-sponsored by The Cyber Threat Alliance. You can register to view the full recordings of the two day event here:

https://events.adaptivemobile.com/hardenstance-ttsi2022

Each speaker and the start-time of their talk in the video recording is listed here:

Day 1

- 0.00.00 Patrick Donegan, (Founder, HardenStance)
- 0.09.25 David Rogers (Chairman, GSMA's Fraud and Security Group – FASG)
- 0.29.26 Kathryn Condello (Senior Director, National Security, Lumen)
- 0.59.44 Cathal Mc Daid (CTO, Enea AdaptiveMobile Security)
- 1.24.44 Przemyslaw Deba (CISO, Orange Polska)
- 1.51.14 Roland Dobbins (Principal Engineer, NETSCOUT)
- 2.15.38 Jaya Baloo (CISO, Avast)
- 2.43.10 Michael Daniel (President and CEO, Cyber Threat Alliance – CTA)
- 3.03.16 Derek Manky (VP Global Threat Intelligence, Fortinet)

Day 2

- 0.00.00 Patrick Donegan (Founder, HardenStance)
- 0.06.45 Omer Koker (Objects Consulting Ltd UK)
- 0.29.10 Erno Doorenspleet (VP, Security Strategy, KPN)
- 0.56.00 Nelson Silva, (Security Product Manager, Nokia)
- 1.21.40 Muddasar Ahmed and Dr. Michaela Vanderveen (MITRE)
- 1.45.08 Manuel Kamp (Head of Cyber Threat Intelligence, Deutsche Telekom)
- 2.00.43 Angel Fernandez (AVP, Security Solutions, Allot)
- 2.26.40 Peter Haigh (Technical Director, Telecommunications, NCSC)
- 2.48.40 Tim Allsopp (Senior Strategy Manager, Telus)
- 3.12.45 Patrick Donegan (HardenStance) & Cathal McDaid (AdaptiveMobile)

More Information

- AdaptiveMobile: "Spectrum of Violence: Mobile Network-enabled Attacks in Hybrid Warfare"
- NETSCOUT Threat Intelligence Report (2H 2021)
- FortiGuard Labs Threat Landscape Report (February 2022)
- Nokia's Threat Intelligence Report 2021
- "Keeping Users Safe in 2022" Allot
- About CISA's Joint Cyber Defense Collaborative (JCDC)

- About Cyber Threat Alliance
- GSMA's T-ISAC home page
- "Using Threat Intelligence in Telecoms (TTIS2021)"
- "Defending Telecoms against Nation State Cyber Threats" (June 2022)
- View comments on the post-TTIS 2022 event blog by speakers Kathryn Condello (Lumen) and Przemyslaw Deba (Orange Polska)

About HardenStance

HardenStance provides trusted research, analysis and insight in IT and telecom security. HardenStance is a leader in custom cyber security research and leading publisher of cyber security reports. HardenStance is also a strong advocate of industry collaboration in cyber security and is the organizer and host of the Telecom Threat Intelligence Summit. HardenStance openly supports the work of key industry associations, organizations and SDOs including NetSecOPEN, AMTSO, The GSM Association, MEF, OASIS, ETSI. The Cyber Threat Alliance. HardenStance is also a recognized Cyber Threat Alliance ‘Champion’.

Register to receive public domain HardenStance reports when they're released

HardenStance Disclaimer

HardenStance Ltd has used its best efforts in collecting and preparing this report. HardenStance Ltd does not warrant the accuracy, completeness, currentness, noninfringement, merchantability or fitness for a particular purpose of any material covered by this report.

HardenStance Ltd shall not be liable for losses or injury caused in whole or part by HardenStance Ltd’s negligence or by contingencies beyond HardenStance Ltd’s control in compiling, preparing or disseminating this report, or for any decision made or action taken by user of this report in reliance on such information, or for any consequential, special, indirect or similar damages (including lost profits), even if HardenStance Ltd was advised of the possibility of the same.

The user of this report agrees that there is zero liability of HardenStance Ltd and its employees arising out of any kind of legal claim (whether in contract, tort or otherwise) arising in relation to the contents of this report.