No.42
September 16th, 2020

HardenStance Briefing

Trusted research, analysis & insight in IT & telecom security

PUBLIC/UN-SPONSORED

An ATT&CK-Like Framework for Telcos

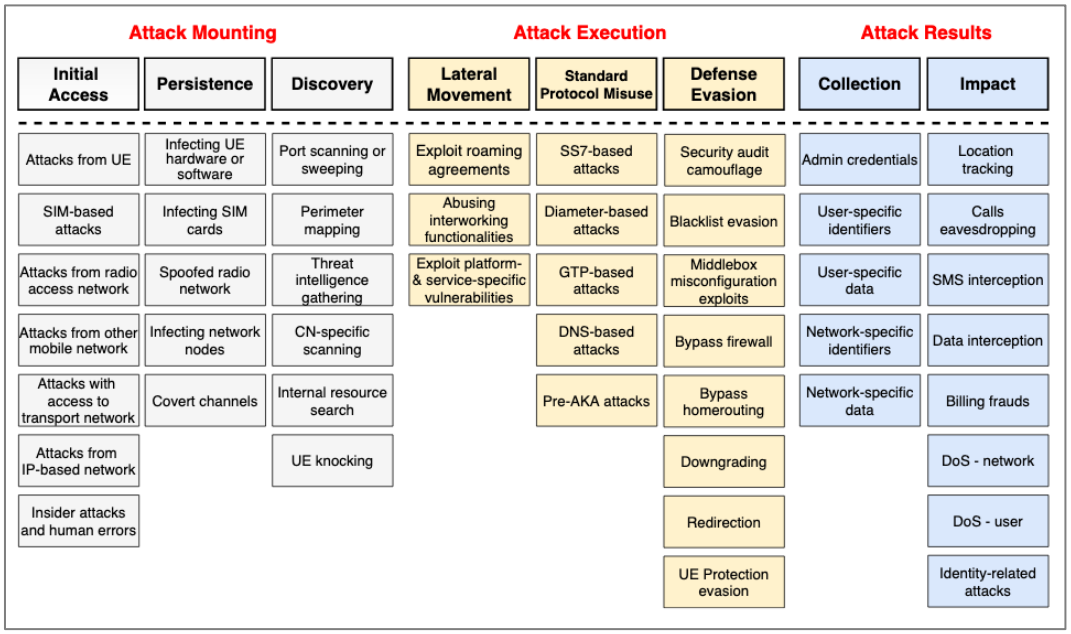
- Two enterprising individuals from Ericsson and Nokia have taken the first steps towards defining an ATT&CK-like Framework for the telecom sector.
- Global political tensions are the primary barrier to better threat intelligence sharing between telcos in different countries. A common ATT&CK-like Framework would help remove secondary - but still critical - technical and operational barriers.
- Within the boundaries set by their regulators, telcos should engage with Ericsson, Nokia and others in this work with a view to potentially leading it over time.
- If this Framework becomes rich enough and widely adopted, it could eventually serve as a guide to vendor selection in telecom security products.

Telcos are already good at threat intelligence sharing at a global level when it comes to maintaining the availability of global Internet services.

HardenStance extends kudos to Jonathan Olsson, RAN Security Researcher at Ericsson and Sid Rao, Core Network Security Researcher at Nokia Bell Labs. During the second quarter, the two of them started putting their heads together on taking MITRE's highly respected ATT&CK Framework for threat intelligence sharing and adapting it to the needs of the telecom sector. A first version is shown in **Figure 1.** It features eight tactics, compared with the eleven that feature in the ATT&CK Framework for the enterprise market (we always have to do things slightly differently in telecom, don't' we?).

Telcos are already good at threat intelligence sharing at a global level when it comes to maintaining the availability of global Internet services. As an example, telcos have a proven framework for sharing threat intelligence and collaborating via major peering points to mitigate the sorts of large-scale Distributed Denial of Service (DDoS) attacks that put many of them, their services, and their customers at high risk all at once.

Figure 1: The First Draft of an ATT&CK-Like Framework for Telecom



Source: Nokia (see "More Information" for the full paper)

Threat Intelligence Sharing: Nowhere Near Where it Should Be

Beyond that, global threat intelligence sharing among telcos is nowhere near where it ideally should be. In advanced countries threat intel sharing tends to be pretty effective at the national level. It tends to be substantially less effective at the regional level and marginally effective at a global level (other than among political allies). Because of this, telcos and their customers continue to suffer from cyber attacks that impacted another telco elsewhere in the world six or twelve months earlier but which the most recent victim was unable to learn from in time to protect themselves.

Politics is the biggest barrier to greater threat intelligence sharing in the telecom sector. Nation states that are carrying out cyber attacks on one another's critical infrastructures – including one another's telecom networks – aren't exactly motivated to trust one another to share cyber threat intelligence in good faith.

Telcos and their customers continue to suffer from cyber attacks that impacted another telco elsewhere in the world six or twelve months earlier.

There is another critical barrier, though. This is the lack of even a basic common language and format with which security professionals in different telcos can describe, classify and share details around the specific threats they see - and share best practice approaches to prevention, detection and mitigation. This is the part of the problem that Jonathan Olsson and Sid Rao are trying to fix, building on the example of the highly respected MITRE ATT&CK Framework which is widely used in enterprise IT security. MITRE is widely hailed for its work in taking very abstract cyber threat models and expressing them in very concrete terms through ATT&CK. This renders it relatively easy for information security professionals to understand, interpret and communicate around cyber threats and develop defensive strategies.

Without a cooling of international cyber hostilities, arriving at an agreed threat modeling framework for telecom won't trigger rapid progress in threat intelligence sharing. Nevertheless, it is a critical enabler. Without it, substantial progress can't be made - even with a more benign global political landscape.

The so-called Tactics Techniques and Procedures (TTPs) that cyber threat actors use to target the telecom environment are necessarily different to those they use to target enterprise IT environments. Here's why:

- The telco network technology environment is unique. You won't find SS7 or GTP in a bank's network. You won't find different RAN, transport and core domains either.
- Telco networks are multi-layered. Think TDM, ATM, Carrier Ethernet and IP/MPLS or 2G, 3G, 4G and 5G. It's long been the case that no two telco networks are architected the same way, using the same technologies. Even more diversity beckons with the greater architectural complexity and flexibility ushered in with 5G.
- Cyber threats targeting telcos don't just exploit vulnerabilities in the telecom network. They also exploit the exact same IT, cloud and mobile device vulnerabilities among internal assets that telcos share in common with other large organizations.

Mapping a Threat Model to Different Operational Realities

Figure 1 gives a very high-level perspective on how threat actors targeting the telecom sector use specific TTPs to navigate their way around telco networks. While this is a good start, it only scratches the surface of what needs doing. The best way to illustrate why is to map **Figure 1's** high level view to the daily reality – or variety of daily realities – experienced in security operations in different telcos around the world. Specifically:

- Telco security teams have to create detailed reports of significant security incidents that impact them – maybe in Word, PowerPoint or Excel. Within some telcos, these reports aren't necessarily all created in the same format, created by one single department, or even stored in one place.
- The nomenclature used to describe an attacker's TTPs may be consistent within that telco or it may not. So long as they are able to give an account of an incident to

their national regulatory agencies that fulfils their obligations under local legislation, that meets their minimum requirements.

- Now pan out from that single telco perspective and consider what this picture looks like from the perspective of a thousand or more telcos and ISPs worldwide and their large vendor partners around the world. Thousands upon thousands of incident reports are being generated in different formats. They cite a huge variety of incidents, describing them all in different ways. Although they may be described differently, some incidents are actually identical to one another. There's a close overlap between many others.

Besides telcos requiring the all-important permission from their governments, mapping even a subset of all this data into a globally shared threat intelligence framework for telcos requires broad industry agreement on the following:

- a robust mechanism for anonymizing a telco's incident report data to comply with data privacy regulations.
- a robust mechanism for anonymizing data without materially devaluing the usefulness of the data to others.
- a common language for describing different security events, including the different steps in the TTPs used.
- a common format for threat intelligence sharing between trusted parties.

Thousands upon thousands of incident reports are being generated in different formats. They cite a huge variety of incidents, describing them all in different ways.

Ultimately, the obvious candidate language and protocol for describing and sharing threat intel is Structured Threat Information Expression (STIX) and Trusted Automated Exchange of Indicator Information (TAXII). These are specified by the Organization for the Advancement of Structured Information Standards (OASIS) Cyber Threat Intelligence (CTI) Technical Committee. These standards are widely used by leading enterprise security teams, by the MITRE ATT&CK Framework, and by organizations like the Cyber Threat Alliance. Adapting STIX would probably require some telco-specific modelling to take account of telco-specific protocols and vocabulary.

Achievements to Date?

It's very early days but here's how far Olsson and Rao have got so far:

- After their first joint presentation to an EU-run event focused on the ATT&CK Framework in May this year, they had responses from around 20 interested parties from other companies voicing their support for the initiative and interest in contributing.
- As shown in **Figure 1**, a first version of a threat intelligence matrix for telecom has been put forward. This comprises 47 different attack techniques as well as 8 tactics.
- Work has started on establishing a format from which to drive continued work on the framework as a community driven effort.
- MITRE wants the effort to develop organically within the telecom sector before deciding whether to commit any of its own resources to it directly.

Operator Engagement is Essential

To gain real-world support in telco security operations, this initiative is going to need substantial direct engagement by the operator community. If sufficient momentum can be built up, the question will arise as to whether this effort should remain independent or whether it should be integrated into a broader industry grouping or association.

The obvious candidate here is the GSM Association. It has been growing its activities in cyber security in the last year or two, including by jointly specifying the Network Equipment Security Assurance Scheme (NESAS) with 3GPP and forming an Information Sharing & Analysis Centre (ISAC) for the telecom sector or T-ISAC.

The Coronavirus Pandemic's impact on Mobile World Congress has dealt a heavy blow to the GSMA's business model. Even if it might theoretically be the right 'home' for this activity, the GSMA's support for even high priority projects can't be taken for granted as it once could.

Within the boundaries set for them by their national governments, telcos themselves should be taking a lead in defining and scoping out this framework.

But even if the GSMA does take it on, that can't be a substitute for direct engagement by individual telecom operators. Within the boundaries set for them by their national governments, telcos themselves should be taking a lead in defining and scoping out this framework. Telco security professionals should be the primary users and beneficiaries of this tool. Ericsson and Nokia should be thanked for triggering this effort but neither they, nor any other vendors, should be left in the driving seat.

A Potential Input into Vendor Selection

As well as assisting day to day telco security operations, an ATT&CK-like Framework for telecom could also serve as a guide to vendor selection of telecom security products. Specifically, it could help telcos better understand how effective different product types, or even different vendor products, are at protecting against specific threats.

The precedent here is the ongoing series of vendor evaluations that MITRE is carrying out on Endpoint Detection and Response (EDR) vendors. These record and openly publish each vendors' performance at detecting the TTPs of specific Advanced Persistent Threat (APT) groups (See 'More Information'). ■

Interested parties should contact jonathan.olsson@ericsson.com & sid.rao@nokia.com

More Information

- jonathan.olsson@ericsson.com and sid.rao@nokia.com
- "Threat Modeling Framework for Mobile Communications Systems" (Sid Rao, Nokia; Silke Holtmanns, Adaptive Mobile; Tuomas Aura, Aalto University)
- The MITRE ATT&CK Framework: https://attack.mitre.org
- "Mitre's ATT&CK Evals are out: Cheers!" (May 2020).
- "New STIX and TAXII Releases Approved" (April 2020)
- The GSMA's T-ISAC: https://www.gsma.com/security/t-isac/
- The Cyber Threat Alliance: https://www.cyberthreatalliance.org/
- "Ericsson & Nokia Complete 5G CyberHack" (February 2020).
- Principal Analyst: patrick.donegan@hardenstance.com
- www.hardenstance.com
- Register for free email notifications whenever HardenStance publishes new content.
- HardenStance received no payment - direct or in-kind - for publishing this Briefing.

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. HardenStance openly supports the work of key industry associations, organizations and SDOs including NetSecOPEN, AMTSO, The Cyber Threat Alliance, The GSM Association, OASIS, ETSI and TM Forum.

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.