IBIMA Publishing
Communications of the IBIMA
https://ibimapublishing.com/articles/CIBIMA/2025/962976/
Vol. 2025 (2025), Article ID 962976, 7 pages, ISSN: 1943-7765
https://doi.org/10.5171/2025.962976

Research Article

Man-in-the-Middle Attacks on the PFCP Protocol in 5G Core Networks and Log-Based Techniques for Their Detection

Krzysztof KOSMOWSKI, Rafal BRYS and Adam DUDKO

Military Communication Institute National Research Institute,
Warszawska 22a 05-130 Zegrze Poludniowe, Poland

Correspondence should be addressed to: Rafal BRYS; rafal.brys@wil.waw.pl

Received date:26 March 2025; Accepted date:13 August 2025; Published date: 17 November 2025

Academic Editor: Jaroslaw Michalak

Abstract

The paper examines the feasibility and implications of Man-in-the-Middle (MitM) attacks on the Packet Forwarding Control Protocol (PFCP) within the 5G Core Network. The study demonstrates how PFCP control messages exchanged between the Session Management Function (SMF) and the User Plane Function (UPF) can be intercepted and modified, enabling an adversary to disrupt or manipulate PDU session establishment and maintenance. Practical implementations of such attacks are presented, illustrating the potential impact on network operation and user data flows. In addition, the paper investigates methods for detecting these threats using log-based analysis. Logs collected from SMF and UPF components were processed and examined to identify anomalies indicative of protocol misuse or unexpected module behaviour. The results highlight critical security vulnerabilities resulting from insufficient PFCP signalling protection and highlight the effectiveness of log-based monitoring techniques in identifying threats in 5G core networks.

Keywords: 5G Core Network, PFCP protocol, packet manipulation.

Introduction

The 5G technology, offering new opportunities for the delivery of services, has sparked justified global interest. As always in such situations, besides the opportunities associated with implementing new technologies, there are also new risks. These risks are the subject of numerous research teams, including the authors of this paper, who report on potential vulnerabilities in the deployed solutions.

The literature reports various classes of threats that may occur in more or less realistic scenarios. When considering a multi-level cyberattack scenario, several levels of access required by an attacker to execute specific attacks can be distinguished. The most fundamental precondition for success is gaining access to the network where communications occur between the gNodeB and the core network (CN). At this stage, it can be assumed that the attacker has obtained access to TLS/SSL (Transport Layer Security/Secure Socket Layer) keys. Having access to the network, it is possible to carry out attacks using intercepted messages transported via the NGAP (NG Application Protocol) protocol, for example.

Cite this Article as: Krzysztof KOSMOWSKI, Rafal BRYS and Adam DUDKO (2025)," Man-in-the-Middle Attacks on the PFCP Protocol in 5G Core Networks and Log-Based Techniques for Their Detection ", Communications of the IBIMA, Vol. 2025 (2025), Article ID 962976, https://doi.org/10.5171/2025.962976

The next level of access assumes the presence of an interface within the network that enables launching an application managing the core network. In this situation, it is possible to perform an attack on the application, such as a brute-force attack, to obtain subscriber information for later use in further attacks. Assuming the attacker has gained access to the servers hosting the core network, fingerprinting the network using standardized 3GPP APIs (Application Programming Interface) becomes possible. The attacker can gain access to one or several network functions and, after compromising them, send messages that can result in service disruption through a Denial-of-Service (DoS) attack or disable specific network functions.

The following sections of this paper present attack vectors on the 5G core network identified in the literature, aligning with the above-mentioned attack philosophy. Subsequently, the paper describes the functions performed by the PFCP protocol within the 5G core network architecture, which serves as an attack vector for the attacks on the 5G core network conducted by the authors of the paper. The final section highlights methods for detecting the symptoms of such attacks.

The main contribution of this work is the presentation of attack concepts, their execution, and a discussion of potential methods for detecting such threats.

Related Work

Bui Nhat Linht's (2023) article presents a study of TLS protocol vulnerabilities in open-source 5G network implementations. The research focuses on analysing TLS vulnerabilities and compliance with 3GPP requirements in three different open-source 5G core networks: free5GC, Open5GS, and OAI 5G CN. The analysis was conducted using automated scanning tools and revealed weaknesses in the examined implementations. Often, exploiting vulnerabilities at the TLS level is a necessary preliminary step to conducting further, multi-stage operations. In the literature referenced below, it is assumed a priori that this security protection has been bypassed.

Salazar et al (2021) described an attack on the UPF network function using the PFCP protocol, which involves manipulating user sessions. The attack assumes access to the N4 interface, enabling unauthorized actions such as requests for the deletion or modification of PFCP sessions, or flooding the system with session establishment requests.

Another attack discussed in the literature is a DDoS (Distributed Denial of Service) attack on signalling presented by Park et al (2022). This attack leverages the fact that the user equipment (UE) registration procedure, completed on the establishment of a tunnel, requires the exchange of numerous messages between different 5G network instances. Generating sufficiently high signalling traffic with appropriately modified UEs can result in blocking some network functions in the core network.

Salazar et al (2021) described also a DoS attack on the AMF (Access and Mobility Management Function) via the NGAP protocol, along with the execution of one of the security tests proposed in the 3GPP specification. The attack utilized an open-source tool called 5Greplay, which allows for packet manipulation.

Anmol et al (2024) identified the risk of DDoS attacks on various 5G network interfaces and proposed a detection solution based on Density-Based Clustering (DBC). They suggest implementing the DBC function on interfaces selected by the administrator. By analysing transmitted packets over time, the solution provides calculated indicators to the DADPF (DDoS Attack Detection and Prediction Function).

Ali Ghubaish et al (2024) propose the use of Hybrid Deep Reinforcement Learning (HDLR) as part of an Intrusion Detection System (IDS). It is located at the edge of the 5G core network (MEC - Multi-access Edge Computing), intended to support IoMT (Internet of Medical Things) infrastructure. This solution, acting as both a network and user IDS, detects attacks such as MiTM, DDoS, Ransomware, and Buffer Overflow.

A different approach is presented by Dudek's (2021) article. The results of an attack executed as part of the PwC & Aalto 5G Cybersecurity Challenge are described. Attackers attempted to achieve their objective with access to the core network only, via an exposed IP interface. After identifying individual network functions, they disrupted network operations by removing certain network functions (which was the goal of the exercise).

Communication between SMF and UPF Network Functions – PFCP Protocol

The aforementioned PFCP protocol is a connectionless protocol transported over UDP. In 3GPP networks, it is used for communication between the Control Plane (CP) and the User Plane (UP). This protocol is unencrypted, making it vulnerable to data modification within packets. A simplified architecture of the 5G Core network, highlighting PFCP communication, is shown in Figure 1.

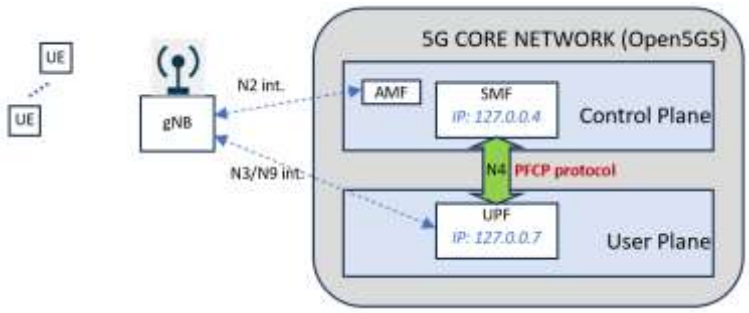

Fig. 1. Communication between the SMF and UPF using the PFCP protocol

Through this protocol, the UPF receives information from the SMF about Packet Detection Rules (PDR), forwarding/routing rules (FAR), Quality of Service (QoS) rules (QER), and Usage Reporting Rules (URR). These are used to establish, remove, or modify GTP-U tunnels between the UE (User Equipment), the UPF, and the Data Network (DN). The tunnels are set using the GPRS Tunnelling Protocol.

Within such packets, no additional session information related to the UE is included; they are used solely for verifying network availability or establishing a connection/association between modules. The Figure 2 shows an example of the exchange of PFCP maintenance messages (heartbeat), captured with the Wireshark tool.

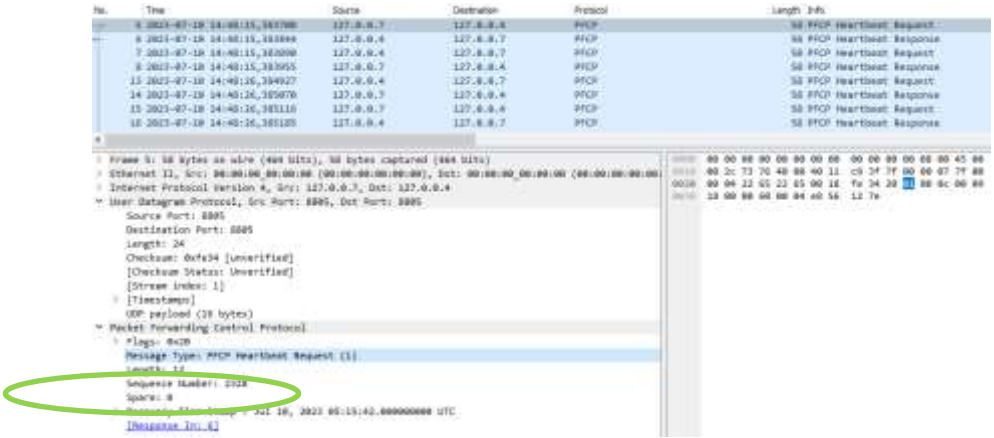

Fig. 2. PFCP protocol - control communication

Other types of messages, identified by values ranging from 50 to 57 (Table 1), are associated with establishing, modifying, and deleting session contexts/tunnels for a specific UE. For session-related messages, in addition to the PFCP protocol header, a list of Information Elements (IE) — including Vendor-specific Information Elements — may be attached. The complete list of PFCP message types is available in the standardization document "LTE; 5G; Interface between the Control Plane and the User Plane Nodes (3GPP TS 29.244 Version 15.8.0 Release 15)" (2020). A fragment is provided below.

Table 1: Selected PFCP message identifiers on N4 interface

Message Type Value (Decimal)	Message
0	Reserved
	PFCP Node related messages
1	PFCP Heartbeat Request
...	
	PFCP Session related messages
50	PFCP Session Establishment Request
51	PFCP Session Establishment Response
52	PFCP Session Modification Request
53	PFCP Session Modification Response
54	PFCP Session Deletion

Concept of Attacks on PFCP

The attacks were carried out in a test environment consisting of implementations: Open5gs as 5G Core Network (5G CN) and srsRAN as a 5G base station (gNB) and user terminal (UE). The 5G CN (its whole modules – network functions) has been launched on the separate terminal. Hence, communication between 5G CN network functions (NF) took place via local interfaces (lo) on this terminal. The base station gNB and the user terminal UE have been launched on another terminal and were connected to 5G CN via local area network (LAN). We assumed that an attacker achieved an administration access (physically or remotely e.g. via SSH) to machine where the 5G CN was placed. The attacks were therefore carried out locally on the 5g CN machine.

Two attacks were planned based on analysing the PFCP protocol session: 1) Deleting sessions between the UPF and UE and 2) Rejecting session establishment requests from the UPF for the UE.

A. Deleting Sessions between the UPF and UE

When the UE initiates connectivity, it first establishes a connection through the Radio Access Network (RAN) to the Access and Mobility Function (AMF), where device registration occurs. After registration is accepted, the connection to the UPF is established. The UPF is controlled by the SMF, with communication enabled by the PFCP protocol.

One type of message useful for the planned attack is the session deletion command, which removes the GTP-U tunnel associated with a session. This typically occurs when the UE disconnects. Notably, even after the GTP-U tunnel for a given UE is removed, the UE remains connected to the RAN, resulting in the inability of the UE to access the DN (e.g., the Internet).

For each Session Deletion Request sent by the SMF, the UPF returns session status information with the appropriate code. The deletion request must include the SEID (Session ID) of the session to be removed. The SEID numbering starts at 1 upon the initialization or restart of the UPF module and increments by 1 for each subsequent session.

This behaviour can be exploited to perform an attack where Session Deletion Requests with incrementally increasing SEID numbers are sent to the UPF. Ultimately, it results in the deletion of all sessions.

B. Rejecting Session Establishment Requests

When the UE attempts to establish a connection to the DN, the SMF sends a Session Establishment Request to the UPF. If the session is successfully established, the UPF responds to the SMF with a status code in the cause field set to 1 (Request Accepted). Following successful session establishment, the SMF sends a Session Modification Request to the UPF, which then sets up the GTP-U tunnel. Upon successful tunnel establishment, the UPF sends a confirmation in a Session Modification Response message.

If the UPF cannot establish the session, the response includes an appropriate cause code along with supplemental information included in "LTE; 5G; Interface between the Control Plane and the User Plane Nodes (3GPP TS 29.244 Version 15.8.0 Release 15)" (2020).

The attack involves modifying the Session Establishment Response PFCP packet sent from the UPF to the SMF. This modification ensures that every attempt of session and tunnel establishment between the UE and UPF is rejected, with the Request Rejected (reason not specified) error code.

C. Attack Execution

The Open5GS environment, available on the https://open5gs.org (2024) web page, was used to perform these attacks. Due to the configuration of our environment—where all 5G Core Network functions are hosted on the same server and use the local IPv4 address range 127.0.0.0/8—the attacks were also executed on this server.

To perform a Man-in-the-Middle attack and manipulate packets, it was necessary to redirect them from the system queue to a separate queue. This was achieved by configuring the iptables firewall as follows:

iptables -I OUTPUT -s 127.0.0.7/32 -d 127.0.0.4/32 -p udp --dport 8805 -j NFQUEUE --queue-num 1

Queue 1 was processed by a script that intercepted, modified, recalculated IP and UDP checksums, and redirected the packets back to the system queue.

Python3 scripts were used with the NetfilterQueue library developed by Fox (2023), for accessing the OS network buffer and the Scapy library available on the https://scapy.net web page, for handling PFCP protocol layers.

PFCP ATTACK – DELETING SESSIONS BETWEEN THE UPF AND UE:

The attack involved modifying every fourth Heartbeat Request packet sent from 127.0.0.4 (SMF) to 127.0.0.7 (UPF). Other packets of this type were left unmodified to avoid completely disrupting communications between the network functions. The attack was executed as follows:

- intercept every fourth PFCP packet with the message_type field set to 1 (Heartbeat Request);
- modify the message_type field to 54 (Session Deletion Request);
- set the SEID field value (incrementing by 1 for each subsequent Heartbeat Request packet);
- remove additional payload data from the packet;
- recalculate IP and UDP checksums and redirect the packet back to the system queue.

PFCP ATTACK – REJECTING SESSION ESTABLISHMENT REQUESTS

The methodology for this attack was similar to the previous one, with the following specific steps:

- redirected packets in queue 1 were verified for the message_type field in the PFCP header set to 51 (Session Establishment Response);
- the payload of the PFCP protocol was searched for the IE_Type field with a value of 19 (indicating the cause field). Its value was then changed from 1 (Request Accepted) to 64 (Request Rejected).

D. Results of the attacks carried out

In the case of running attacks described in A (deleting of existing PDU sessions), the confirmation of attack effectiveness was information in the UPF logs. Log entries showed session deletion events and no active sessions, as confirmation of a successful attack:

07/12 09:29:06.284: [upf] INFO: [Removed] Number of UPF-sessions is now 0 (../src/upf/context.c:212).

In the meantime, the log entries from SMF module informing about session deletion requests have been presented, like:

07/12 09:27:57.755: [smf] DEBUG: Session Deletion Request (../src/upf/n4 handler.c:461)

A large number of such entries may be a signal about malicious activity. Since the attacker didn't know the SEIDs of active PDU sessions, subsequent sessions with increasing ID were deleted. Therefore, if he requested the deletion of a non-existent session, an error entry appeared in the UPF logs, like:

07/12 09:27:57.755: [upf] ERROR: No Context (../src/upf/n4-handler.c:464)

It informed about an attempt to delete a non-existent PDU session. Again, a large number of such entries as a result of session deleting request are a clear signal of an attack.

Similar verification of the correctness of the attack described in B (rejecting session establishment request) was performed. During the attack, entries in the SMF logs confirming the rejection of session establishment requests were recorded:

07/10 09:22:31.963: [smf] ERROR: PFCP Cause [64]: Not Accepted (../src/smf/n4-handler.c:179).

User terminal UE, in case of rejecting PDU session establishment, tried to establish it anyway. As a consequence, the above entries appeared in a large number in the short time period (Fig. 3). Such events again indicate an anomaly and may suggest attack attempts. Additional analysis of the causes of errors may be helpful in assessing the situation.

Attack Symptoms Detection

The traces of the attacks described above are difficult to detect and must be searched for in the log files of individual network functions. Analysing the course of the attacks and monitoring possibilities, it can be concluded that an attack targeting the rejection of PDU session establishment, similarly to attacks that remove sessions, is not easy to detect. It seems reasonable to monitor the indicators, such as the number of PFCP protocol errors reported by both the SMF and UPF.

A verification of the ability to use Prometheus and Grafana as tools to identify attacks was conducted. For this purpose, appropriate scripts were developed. These scripts performed such actions: analysed log files, counted the occurrence of errors and session modification or deletion, and reported events to Prometheus. Example results of PFCP attack – rejection sessions requests from UE are presented in Fig. 3. Red arrows indicate an increase in the number of monitored events (PFCP errors occurring in SMF logs) indicating attacks on the PFCP protocol signalling.

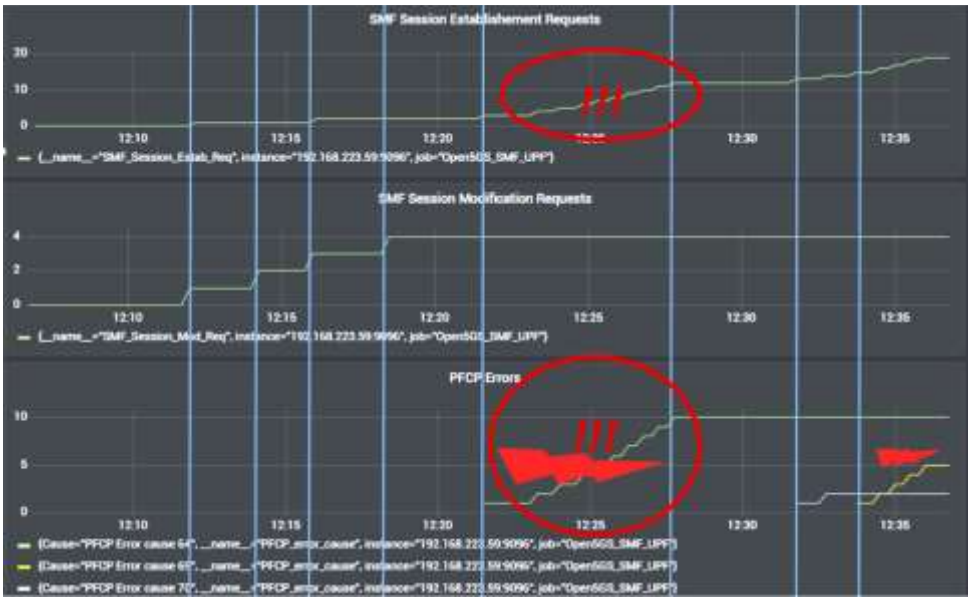

Fig. 3. Symptoms of session establishment rejection attacks reported by the SMF function

An exponentially increasing number of PDU session establishment requests from the same UE (as the UE anyway tried to establish PDU session), combined with a concurrent rise in the number of errors, may indicate anomalies in the 5G core network. This indicates that some UE is trying to establish a PDU session, and these attempts are falling. By analysing the cause of the errors, it can be determined whether the UE is establishing a session with incorrect data, or the requests are being rejected due to an attack. Individual and difficult-to-detect session deletion attacks can be signalled by the occurrence of two factors simultaneously: the appearance of "PDU session deletion request" messages and information in the UPF module logs regarding erroneous contexts for such messages, labelled as "No context errors."

Summary

The paper presents vulnerabilities of the 5G backbone network reported in the literature that could serve as vectors for cyberattacks. After analysing the sequence of PFCP protocol message exchanges, two attacks were conducted, resulting in the UE not having access to the data network despite being associated with the gNB.

The next element of the research was the analysis of the possibility of recognizing symptoms of such cyberattacks. For this purpose, Prometheus/Grafana tools were used. The appropriate selection of monitored indicators, in this case, taken from system logs, enabled the identification of undesirable events. The indicators presented in the study seem to be useful, and their visualization can help network supervisors assess the situation, identify events, and counteract them. The alarm mechanism of the

Grafana software used in the research provides a range of possibilities for detecting changes in individual indicators as well as correlating changes in several indicators simultaneously. This approach was sufficient in the research work and was ultimately automated.

However, in the case of more sophisticated attacks on 5G networks, this may not be sufficient to automate this process without the knowledge and experience of the operator. It seems that it would be advisable to use more advanced mechanisms of disturbance detection, such as machine learning or artificial intelligence algorithms. These mechanisms would be able to detect intentional events among the identified ones.

The presented types of attacks require access to the communication network for SMF and UPF. The 5G CN modules may be placed on one machine or distributed e.g. in the cloud network. As we pointed out in the IV, the MitM attack should be performed to get access to PFCP packet exchange. For this reason, for system secure against such threat, communication stream should be protected, e.g. using TLS/SLS protocol, in case of distributed CN modules. Even if an attacker redirects the data stream, he will not be able to read the contained information and manipulate it. Unless he gains access to the cryptographic keys. In case of modules placed on one machine, the access to them should be protected also in remote way in particular to the administration privileges.

References

- Ali Ghubaish, Zebo Yang, Raj Jain, (2024), "HDRL-IDS: A Hybrid Deep Reinforcement Learning Intrusion Detection System for Enhancing the Security of Medical Applications in 5G Networks", 2024 International Conference on Smart Applications, Communications and Networking (SmartNets), ISBN:979-8-3503-8532-8 28-30 May 2024, Harrisonburg, VA, USA.
- Amponis, G., et all., (2022), "Threatening the 5G Core via PFCP DoS Attacks: The Case of Blocking UAV Communications." EURASIP Journal on Wireless Communications and Networking 2022, no. 1, [Online], [Retrieved June 2024],) https://doi.org/10.1186/s13638-022-02204-5.
- Anmol Agarwal, Rakshesh P. Bhatt, Clifton Fernandes,(2024), "End-to-End System Level Solution for DDoS Attack Detection and Prediction for 5G and Future Wireless Networks", 2024 International Conference on Smart Applications, Communications and Networking (SmartNets), ISBN:979-8-3503-8532-8 28-30 May 2024, Harrisonburg, VA, USA.
- Bui Nhat Linh, A., (2023), "Analysing Open-Source 5G Core Networks for TLS Vulnerabilities and 3GPP Compliance." RADBOUD UNIVERSITY, [Online], [Retrieved June 2024], https://www.cs.ru.nl/bachelors-theses/2023/Alex_Bui_Nhat_Linh___1040308___Analysing_open-source_5G_core_networks_for_TLS_vulnerabilities_and_3GPP_compliance.pdf.
- Dudek, S., (2021), "Intruding 5G SA Core Networks from Outside and Inside." Penthertz (blog), [Online], [Retrieved June 2024], https://penthertz.com/blog/Intruding-5G-core-networks-from-outside-and_inside.html.
- Fox, M., (2023), "NetfilterQueue: Python Bindings for Libnetfilter_queue." POSIX :: Linux, Cython, Python. [Online], [Retrieved September 2023], https://github.com/oremanj/python-netfilterqueue.
- "https://Open5gs.Org/.", [Online], [Retrieved June 2024], https://open5gs.org/.
- "LTE; 5G; Interface between the Control Plane and the User Plane Nodes (3GPP TS 29.244 Version 15.8.0 Release 15)" (2020), 3GPP, [Online], [Retrieved June 2024], TS 129 244 - V18.9.0 - LTE; 5G; Interface between the Control Plane and the User Plane nodes (3GPP TS 29.244 version 18.9.0 Release 18).
- Park, S., Byungsun Ch., Dowon K., and Ilsun Y., (2022), "Machine Learning Based Signaling DDoS Detection System for 5G Stand Alone Core Network." Applied Sciences 12 no. 23, [Online], [Retrieved June 2024],, https://doi.org/10.3390/app122312456.
- Salazar, Z., Huu Nghia N., Wissam M., Ana R. Cavalli, and De Oca, E.M., (2021), "5Greplay: A 5G Network Traffic Fuzzer - Application to Attack Injection." In Proceedings of the 16th International Conference on Availability, Reliability and Security,, ISBN: 978-1-4503-9051-4 17 August 2021, Vienna, Austria, 1-8., https://doi.org/10.1145/3465481.3470079.
- "Scapy.", (2024), [Online], [Retrieved Septemper 2024], https://scapy.net/.