Malicious RFC standards – ongoing threat

Threat Alert - TA 20-420 - Date: 01/04/2020 - Version: 1.0

TLP:WHITE

	Category	Type	Threat Level	Domain	Sector	Confidence
FOR AMUSEMENT	Hacktivist	Personal Data targeting DDoS	High	World	Any	A1

Key Points

- The established and well-documented threat actor IETF (aka APT0) is likely to strike globally today.
- Its historical activity of introducing malicious standards into internet technology borders on the ridiculous.
- Potential victims should scan their mail traffic for so-called RFC documents issued with today's date and delete them immediately.

Summary

Today, a threat actor known as the Internet Engineering Task Force (IETF), aka APT0, is likely to globally strike against organisations with the goal of disrupting their functioning. This group is said to persistently cause harm to organisations' networks through the periodic publication of malicious RFCs[1] intended to either collect information on users, disrupt services or introduce standards that would utterly exhaust the implementer's resources. Reports of this group's malicious activity can be traced back to 1978, possibly making this actor the first reported Advanced Persistent Threat (APT).

It must be stated that many technological domains are mastered by APT0. In 1989, RFC1097 secretly introduced into the Telnet protocol (an internet standard mostly heard cited by so-called 'Boomers'[2]) the possibility of sending subliminal messages to the users in an attempt to covertly influence their behaviour. In 2010, the threat actor introduced a so-called 'Packet Mood' for TCP packets, allowing TCP packets to have 1 of 12 moods, including Happy, Sad, Frustrated, Angry. Although at first this 'Packet Mood' did not cause much disturbance (it was mostly ignored by network devices), the rise in Millennial users on the internet has set almost all packet moods to Frustrated, leading to conflicts inside UTP cables.

Overall, this threat actor undertakes a wide range of sabotage attempts, ranging from reverse HTTP requests in RFC8565 (users send an answer to a web server expecting the server to send the correct question) up to crafting individual network packets in RFC6592. In this last example, dealing with Null packets, the concept of Denial of Denial of Service is introduced, where Denial of Service is denied to the sender due to inexistence of a packet. According to CERT-EU's assessment, network equipment attempting to find Null packets may possibly come in a state of Denial of Service should the device be patched for the Burden of Proof[3] error, a vulnerability where absence of proof and proof of absence are confused.

Likely in an attempt to use the hot topic of 'Green IT', APT0 issued a 'Scenic Routing for IPv6' RFC7511, sending IPv6 packets[4] over wireless connections rather than dark cables in the ground, allowing for the packets to "get as much clean air and sunlight as possible". The RFC even proposes a combination with RFC1149, which introduced the possibility of transporting IP packets over avian carriers (pigeons) in 1990. This last malware actually ran undetected for 19(!) years until it was picked up by South Africa's Telkom[5]. It was subsequently removed, reportedly because of cloud storage issues in the Dovecot mail server after version v.1.2.4 and refusal to put more than 1 pigeon in a pigeonhole[6].

More recently, in 2019 APT0 has tried to boldly introduce personal data stealing options into the DNS standard in RFC8567. Credential harvesting, credit card data harvesting and social security number harvesting are among the far-ranging capabilities of this malware. Harvested data is encrypted using ROT26[7], an encryption standard long deprecated due to an extremely high rate of cleartext-ciphertext collision.

Comment

As this threat actor has shown its persistence and advanced capabilities, CERT-EU closely monitors any of its activity and will happily receive any and all reporting of APT0 activity through the usual communication channels.

---

[1] Request For Comment, a document used to regulate standards on the internet. See: https://en.wikipedia.org/wiki/Request_for_Comments

[2] This reference is often made in combination with an alleged 'modem' device that made weird sounds when connecting. CERT-EU is not aware of any elements corroborating the existence of such apparatus and considers it highly unlikely it ever existed.

[3] https://www.qcc.cuny.edu/socialsciences/ppecorino/phil_of_religion_text/CHAPTER_5_ARGUMENTS_EXPERIENCE/Burden-of-Proof.htm

[4] IPv6 is likely a hoax not unlike the internet connection device in reference 3. No usage in the wild of IPv6 has yet been reported to CERT-EU.

[5] https://www.reuters.com/article/us-safrica-pigeon/pigeon-transfers-data-faster-than-south-africas-telkom-idUSTRE5885PM20090910

[6] https://medium.com/cantors-paradise/the-pigeonhole-principle-e4c637940619

[7] http://rot26.org/