Russian Attacks Against Singapore Spike During Trump-Kim Summit

By Authors & Contributors

Archived: 2026-04-06 01:06:39 UTC

It's no secret Russia has been launching a steady barrage of coordinated cyber-attacks against the U.S. as many sanctions have been issued against Russian officials and businesses since the 2016 Presidential election.1 Beyond official sanctions, the US-Cert issued an alert in April regarding Russia maintaining persistent access to small office and home office routers warning of widespread espionage. From June 11 to June 12, 2018, F5 Labs, in concert with our data partner, Loryka, found that cyber-attacks targeting Singapore skyrocketed, 88% of which originated from Russia. What's more, 97% of all attacks coming from Russia during this time period targeted Singapore. We cannot prove they were nation-state sponsored attacks, however the attacks coincide with the day President Donald Trump met with North Korean President Kim Jong-un in a Singapore hotel. The attacks targeted VoIP phones and IoT devices, which appears to be more than a mere coincidence.

- Russia accounted for 88% of the attacks against Singapore on 6/12/2018.
- The attack began out of Brazil targeting port SIP 5060, which is used by IP phones to transmit communications in clear text; this was the single most attacked port.
- Following this initial phase, the attacks were primarily reconnaissance scans from the Russian IP address 188.246.234.60, targeting a variety of ports.
- The number two attacked port was Telnet, consistent with IoT device attacks that could be leveraged to gain access to or listen in on targets of interest.
- Other ports attacked include the SQL database port 1433, web traffic ports 81 and 8080, port 7541, which was used by Mirai and Annie to target ISP-managed routers, and port 8291, which was targeted by Hajime to PDoS MikroTik routers.

June 12, 2018 Attacks

Approximately 40,000 attacks were launched between 3:00 p.m. UTC on 6/11/2018, and lasted through 12:00 p.m. UTC on 6/12/2018. That translates to 11:00 p.m. through 8:00 p.m. Singapore time on June 12, the day President Trump met with Kim Jong-un in Singapore.2

Figure 1. Timeline of Singapore attacks

Ninety-two percent of the attacks collected were reconnaissance scans looking for vulnerable devices; the other 8% were exploit attacks. Thirty-four percent of the attacks originated from Russian IP addresses. China, US, France, and Italy round out the top 5 attackers in this period, all of which launched between 2.5 to 3 times fewer

attacks than Russia. Brazil, in the sixth position, was the only other country we detected launching SIP attacks alongside Russia.

Figure 2: Top 10 attack source countries worldwide, June 12, 2018 — Singapore time

Singapore was the top destination of the attacks by a large margin, receiving 4.5 times more attacks than the U.S. or Canada. Singapore is not typically a top attack destination country; this anomaly coincides with President Trump's meeting with Kim Jong-un.

Figure 3. Top 10 attack destination countries, June 12, 2018 — Singapore time

Russia was the primary source of the attacks against Singapore during this period, launching 88% of the attacks. Brazil was the number two attacker, launching 8% of the attacks against Singapore, and Germany was number three with 2% of the attacks. No attempt appears to have been made to conceal the attacks launched from Russia. There was also no malware associated with the attacks against Singapore from Russia.

Figure 4. Top 10 source countries of Singapore attacks, June 11, 2018 through June 12, 2018

Top Attacking Russian IP Address

The majority of the attacks coming from Russia were reconnaissance scans coming from one IP address: 188.246.234.60. The IP is owned by ASN 49505, operated by Selectel. The recon scans were preceded by the actual attacks against port 5060 that came primarily from Brazil.

Attack Destination Ports

The following ports in order of prevalence were targeted in the Singapore attacks:

5060 — clear text Session Initiation Protocol (SIP)

23 — Telnet remote management

1433 — Microsoft SQL Server database

81 — Alternate web server port for host-to-host communication

7547 — TCP port used by ISPs to remotely manage routers via the TR-069 protocol

8291 — Remote management port commonly used by MikroTik routers

8080 — Alternate web server port often used for a proxy server or caching

The SIP port 5060 received 25 times more attacks than port 23 in the #2 position. SIP is an IP phone protocol, and port 5060 is specifically the non-encrypted port versus port 5061, which is encrypted. It is unusual to see port 5060 as a top attack destination port. Our assumption is that the attackers were trying to gain access to insecure phones or perhaps the VoIP server. Attacks against this port haven't been in the news since 2011 when the SIPVicious VoIP tool was popular.[3]

Telnet is the most commonly attacked remote administration port by IoT attackers. It's very likely these attackers were looking for any IoT device they could compromise that could provide them access to targets of interest, which would then enable them to spy on communications and collect data.

Port 7457 is used by ISPs to remotely manage their routers. This protocol is targeted by Mirai and Annie, a Mirai spinoff that caused millions of dollars of damage to European ISPs in late 2016.[4] If any devices in Singapore had this port open and were protected with default admin credentials, it is likely the attackers gained access and used man-in-the-middle attacks to intercept traffic through those devices, collecting data, redirecting traffic, and so on.

Port 8291 was recently attacked by Hajime,[5] the vigilante thingbot created to PDoS devices that would otherwise be infected by Mirai.[6] If any devices in Singapore were listening on this port, and protected with vendor default credentials, it is likely the attackers could have gained access.

Conclusion

It is unclear what the attackers were after with the SIP attacks or whether they were successful. We will continue to analyze the attack data we have collected and update this story as we make new discoveries.

We do not have evidence directly tying this attacking activity to nation-state-sponsored attacks, however it is common knowledge that the Russian government has many contractors within Russia doing their bidding, and that a successful attack on a target of interest would make its way through to the Kremlin.

In regard to mitigating the threat of these types of attacks which, in this case, involved IoT devices and databases directly touching the Internet, our advice is to always:

- Protect remote administration to any device on your network with a firewall, VPN, or restrict to a specified management network. *Never* allow open communication to the entire Internet.
- Always change vendor default administration credentials.
- Stay up to date with any security patches released by the manufacturer.
