Simjacker

Next Generation Mobile Threat

AdaptiveMobile Security Threat Intelligence Unit (TIU), a team renowned for identifying and taking down the very latest mobile threats, has uncovered a new, highly-complex vulnerability that is already being exploited by sophisticated attackers globally. “Simjacker” is a next generation mobile core network attack, capable of obtaining sensitive information and controlling devices in operators who do not have active monitoring and blocking, and who trust in inadequate ‘standard’ security systems. Multiple types of threats are possible using Simjacker, and as this vulnerability is linked to a technology embedded on SIM cards, there is a potential for all types of mobile phones to be attacked.

Background

AdaptiveMobile Security’s industry leading TIU team has detected unusual activity over messaging and signalling bearers in specific customers, occurring over a long period of time.

Specific, targeted subscribers were receiving SMS messages that were causing them to send another SMS with location/terminal information, without any notification or knowledge.

Subsequent deeper investigation revealed a vulnerability that allowed almost every single mobile device in affected operators to be open to manipulation.

We believe this vulnerability has been exploited for at least the last two years by a highly sophisticated attacker group.

How the attack works

The main Simjacker attack involves a SMS containing a specific type of spyware-like code being sent to a mobile phone, which then instructs the SIM Card within the phone to ‘take over’ the mobile phone to retrieve and perform sensitive commands.

The attacks exploit the ability to send SIM Toolkit Messages and the presence of the S@T Browser on the SIM card of vulnerable subscribers. (The S@T Browser is normally used for browsing through the SIM card.)

The Attack messages use the S@T Browser functionality to trigger proactive commands that are sent to the handset. The responses to these commands are sent back from the handset to the SIM card and stored there temporally. Once the relevant information is retrieved from the handset, another proactive command is sent to the handset to send an SMS out with the information.

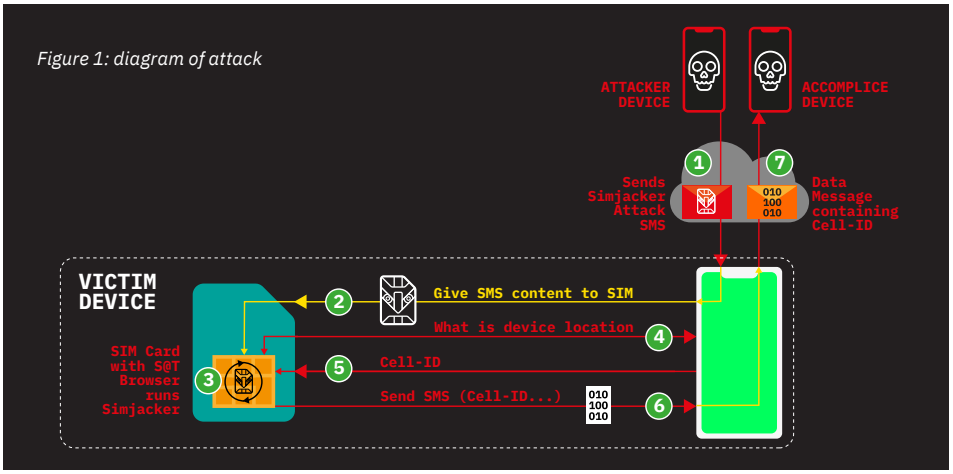
Who is doing this and why

Using SIGIL (Signalling Intelligence Layer), our industry-first global threat analytics system, allowed us to correlate the Simjacker sources with known malicious threat actors.

As a result, we can say with a high degree of certainty, that the source is a large professional surveillance company, with very sophisticated abilities in both signalling and handsets.

These types of companies exploit the fact that some mobile operators may incorrectly regard core network security as solved if they deploy a standard GSMA ‘compliant’ firewall.

Figure 1: diagram of attack



Scope of Vulnerability

AdaptiveMobile Security research indicates that the Simjacker vulnerability could extend to over 1 billion mobile phone users globally, potentially impacting countries in the Americas, Africa, Europe, the Middle East and indeed any region of the world where this SIM card technology is in use. The issue is that in affected operators, the SIM cards do not check the origin of messages that use the S@T Browser, and SIMs allow data download via SMS.

Other types of attacks are also possible using the S@T Browser, including: location tracking, fraud, denial of service, malware spreading and call interception.

We have seen many of these potential attacks being tested and used by the attacker group.

Recommendations for Mobile Operators

Investigate if you have SIM cards with S@T Browser technology deployed in your network and if so whether any S@T Browser-specific proprietary security mechanisms can be applied.

Determine whether your existing network equipment can be configured to filter binary SMS messages from unauthorised sources. You should consider if your current firewall is simply only GSMA document 'compliant'. These GSMA documents should really only be used as a starting point for more effective protection.

Review the ongoing investigation and research you are doing on what is being encountered in your network. Simjacker is just the first (known) next generation mobile core network attack. We have strong indications of other types of innovative techniques being used.

AdaptiveMobile can provide next generation threat intelligence for your network along with industry leading solutions utilising in-network proprietary algorithms to constantly hunt for, identify and enable blocking of suspicious new threat types across messaging and signalling bearers.

Disclosure and Next Steps

AdaptiveMobile Security have submitted details of the exploit to the GSMA as a Vulnerability Disclosure, along with intelligence and recommendations on how to mitigate the attacks.

AdaptiveMobile Security will continue to research how the attacks function, look for other variants of the Simjacker exploits and use of the vulnerability, and investigate related attacks which bypass vulnerable operators.

Further details on Simjacker are available on **www.simjacker.com**

Contact us on
www.adaptivemobile.com/contact-us

About AdaptiveMobile Security

Protecting nations, networks and subscribers, AdaptiveMobile Security is a world leader in cyber-telecoms security, everyday protecting over 2.2 billion people globally from fraudsters, criminals and nation states. Powered by our internationally respected core expertise and foundation in security, AdaptiveMobile Security brings a unique focus on real-time mobile network enforcement. The global insight provided by our security specialist teams and our world-leading Threat Intelligence Unit, combined with our proprietary, telecom-grade Network Protection Platform, ensures AdaptiveMobile Security are trusted by the world's largest service providers and governments to secure their critical communications infrastructure. AdaptiveMobile Security was founded in 2006 and is proud to count the world's largest mobile operators as customers and the leading security and telecom equipment vendors as partners. The company is headquartered in Dublin with offices in North America, Europe, South Africa, Middle East and Asia Pacific.

Head Office

Ferry House, 48-52 Lower Mount St, Dublin 2.
Contact: sales@adaptivemobile.com

Regional Sales Contact Numbers

US, Canada, Latin America Sales: +1 972 377 0014
UK Sales: +44 207 049 0421
Middle East Sales: +97144 33 75 83
Africa Sales: +27 87 5502315
Asia Sales: +65 31 58 12 83
European Sales: +353 1 524 9000

Regional Operational Support Contact Numbers

UK: +44 208 114 9589
Ireland: +353 1 514 3945
India: 000-800-100-7129
US, Canada: +1 877 267 0444
LATAM: +525584211344

www.adaptivemobile.com

MAAWG
MESSAGING ANTI-ABUSE WORKING GROUP

GSMA

IWF Member
DO the right thing