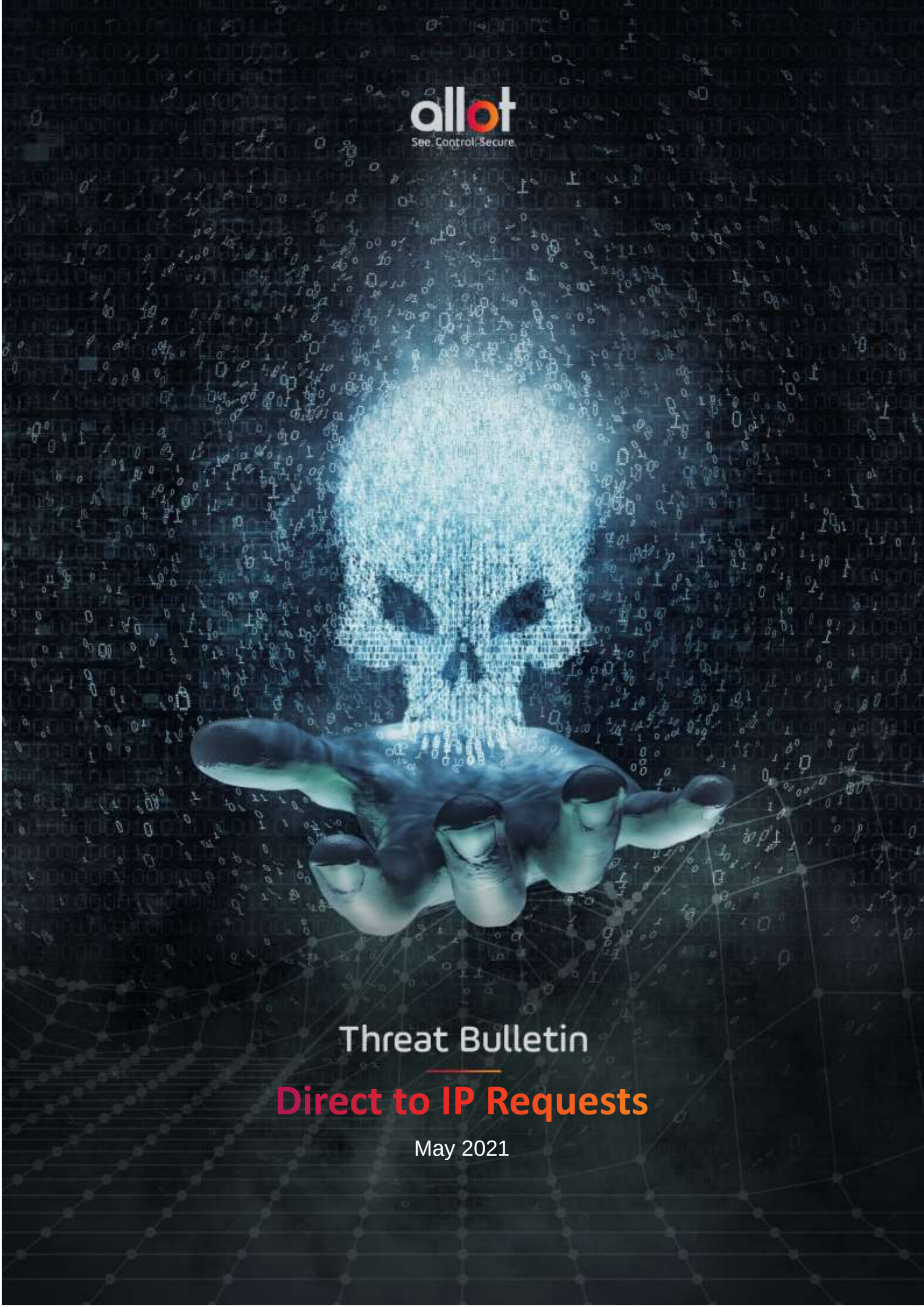


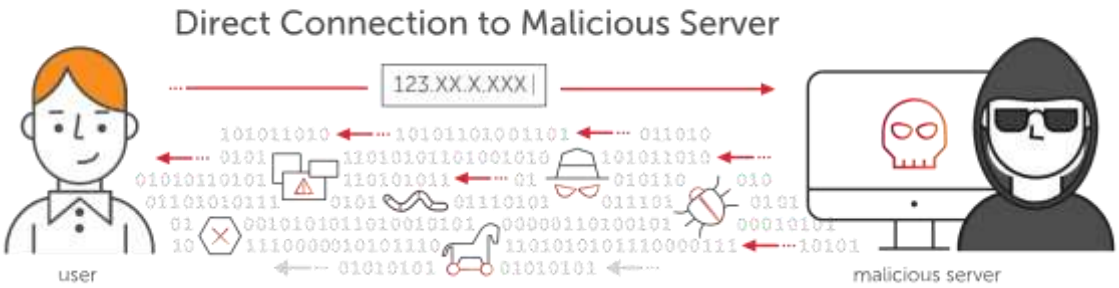
Threat Bulletin

Direct to IP Requests

May 2021

Direct to IP Requests

In recent months, Allot Secure has detected 200% increase in direct requests to malicious IP addresses. Prior to June 2020, most of the Internet connection requests identified and blocked as malicious by Allot NetworkSecure were in the form of domains or URLs, only ~2-4% were direct to IP address requests. Suddenly in the second half of 2020 their volumes started increasing dramatically. By February 2021, direct to IP requests accounted for 14% of all blocks. This increase in attempts to connect to malicious IPS was caused by Android Trojans and other malware trying to connect to their command & control (C2C) servers, phishing, spamming, DDoS attacks and password cracking and login attempts.



How are Users Infected?

Direct to IP requests can originate in all the same ways a regular URL website request does. Users may receive them as links in emails or messaging platforms. The two most proliferous Android Trojans were Joker and Cerberus. Cerberus and Joker both infect users via email attachments, malicious online advertisements, social engineering, deceptive applications, and scam websites. Joker also managed to spread via infected mobile apps that managed to slip past Google's rigorous testing to reach the platform's official app store. Many types of malware include instructions to establish connections directly with an IP controlled by the cybercriminals. Communication with IPs is often done in the background, without the user's knowledge.

Malicious Activity

Spammers and Phishers can replace malicious domains with direct IP addresses of their host sites. The recent increase in direct to IP requests could also be caused by malware attempting to connect with an external command and control (C&C) server. Malicious code often includes instructions to connect directly with an IP controlled by cybercriminals to receive further instructions, exfiltrate sensitive data or carry out a ransomware, botnet or DDoS attack.

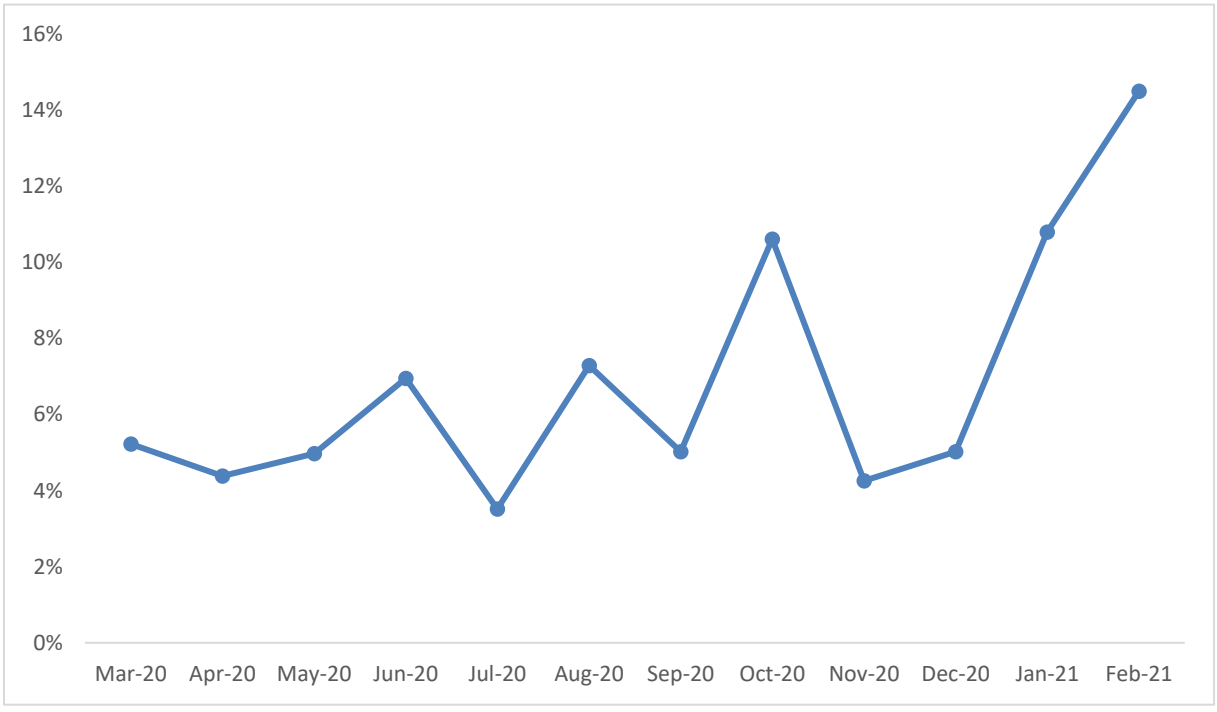
Mobile Trojans (Cerberus, Joker), are capable of intercepting private messages and login credentials, silently signing users up for premium SMS services etc.), hijacking accounts, fraudulent purchases, and text messages.

Allot Secure Malicious IP Blocks

Allot NetworkSecure works at the level of the internet connection to analyze, detect and block access to any malicious web address without the need to send traffic out to a 3rd party tool. Therefore, direct calls to malicious IP addresses are easily blocked to keep users safe.

In the last 12 months, Allot Secure protected users from connecting directly to malicious IPs 68,852,432 times.

Allot Secure IP Blocks as % of all Blocks: Mar 20 – Feb 21

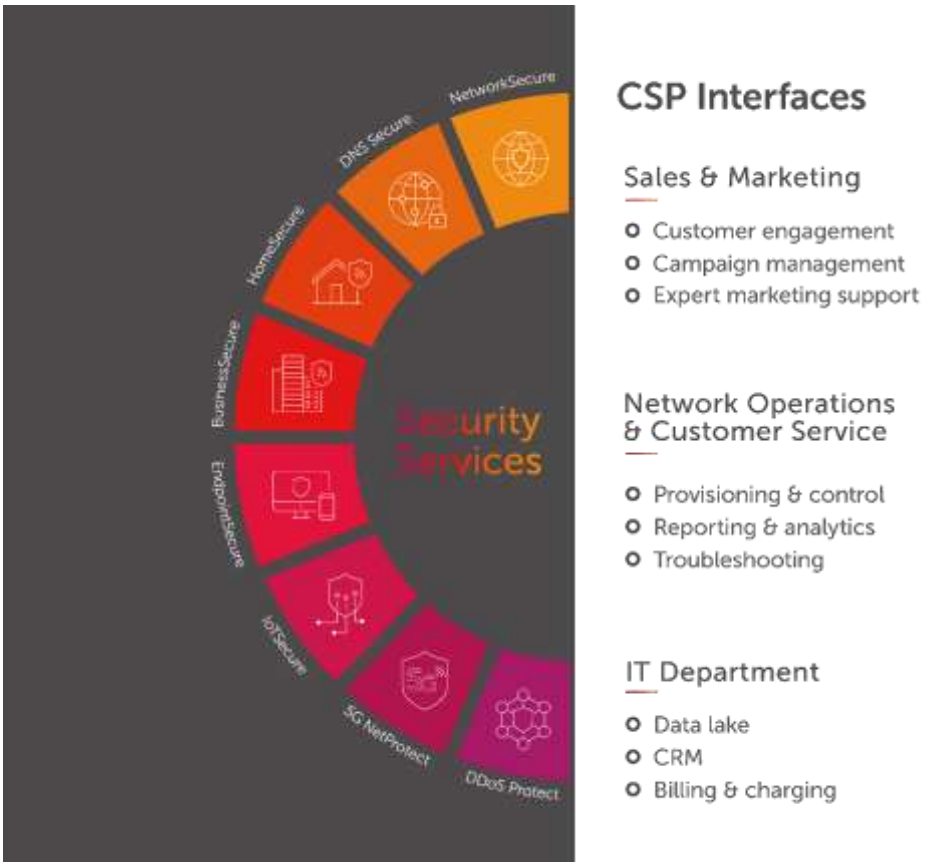


Conclusion

Protect Subscribers with Allot Secure

Allot Secure allows CSPs to protect their subscribers from all types of cyberthreats by offering security as a service (SECaaS) from the network. Up-to-date threat intelligence and in-line anti-virus scanning protects users from connecting to C&C servers, malicious browser trackers, and all types of malware, banking Trojans, crypto jacking, ransomware, and IoT specific attacks such as Mirai and its variants.

Allot Secure unifies network-based security, home and business gateway security and security clients into the CSP's own branded security service. It delivers a seamless customer experience through a single interface for policy setting, reporting, and event handling.



To learn more about how service providers can increase customer satisfaction, NPS and ARPU by offering Allot Network Security Solutions, download the Telco Security Trends Report:

How Effective are CSP Security Services for the Mass Market?
or watch this video: **How Allot NetworkSecure Works**.