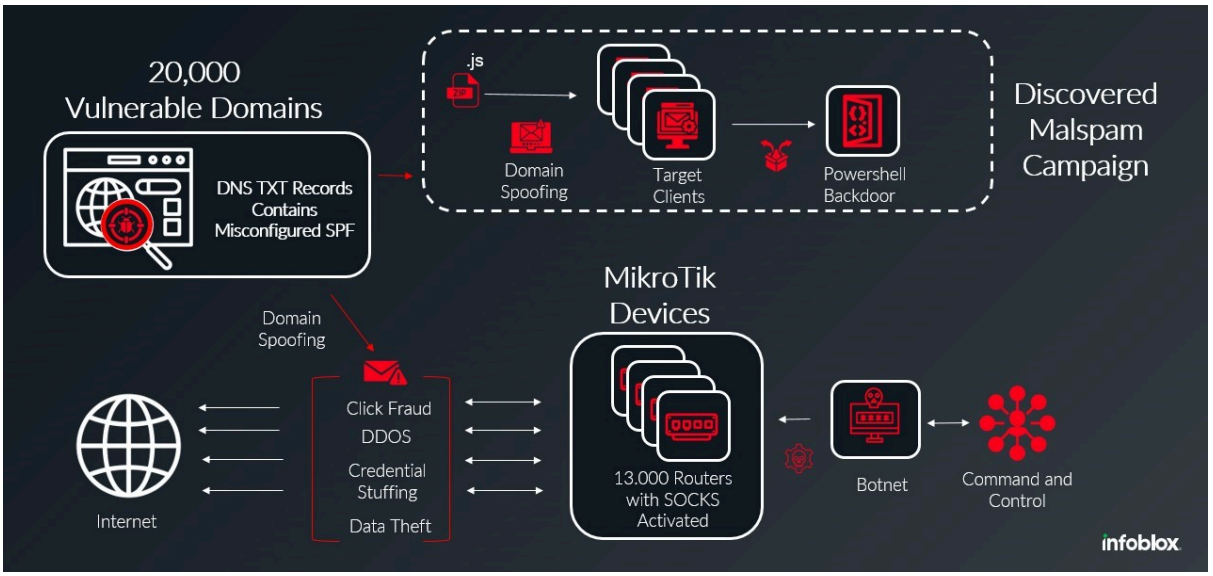
An advanced botnet that launches widespread spam campaigns by utilizing a vast network of Mikrotik routers that have been compromised.

For the purpose of gaining initial access, the botnet that is estimated to have infected approximately 13,000 devices across the globe took advantage of a critical vulnerability in Cisco routers.

Once compromised, these routers were secretly configured as SOCKS proxies that effectively transformed them into a hidden network capable of masking the true origin of malicious traffic.

Because of this infrastructure, the botnet was able to send malicious emails that were disguised as legitimate business correspondence. For example, the botnet could send invoices from shipping companies like DHL's.

These e-mails contained deceptive attachments that were typically ZIP files and concealed malicious JavaScript code that was designed to download and execute a Trojan payload.



DNS Misconfiguration Fuels Large Botnet Operation

The execution of this trojan resulted in the establishment of a covert connection to a command-and-control (C2) server that was connected to previous cybercriminal activity that originated from Russia.

The exploiting of DNS records that were incorrectly configured was a significant contributor to the success of the botnet. An attacker targeted domains with improperly configured Sender Policy Framework (SPF) records.

These misconfigurations that are often unintentional allow any server to send emails on behalf of legitimate domains and effectively bypass email authentication mechanisms like SPF, DKIM, and DMARC.

The botnet was able to impersonate legitimate sender addresses as a result of this, which consequently increased the likelihood that malicious emails would reach their intended recipients.

A widespread compromise of Mikrotik routers highlights the critical importance of robust network security measures, including regular security audits, timely firmware updates, and the implementation of strong access controls.

Organizations need to diligently review and maintain proper DNS configurations and ensure that SPF records are correctly configured to prevent email spoofing and enhance the security of their email communications.

According to Infoblox, the botnet uses more than 13,000 compromised MikroTik devices as SOCKS4 relays in order to launch a campaign of malicious spam.

It exploits DNS SPF misconfigurations and bypasses email protections that enable a wide range of attacks, including DDoS and data theft, highlighting the critical need for secure device configurations and robust security audits.