Iran-Based Threat Actor Exploits VPN Vulnerabilities
(CSB20-16)

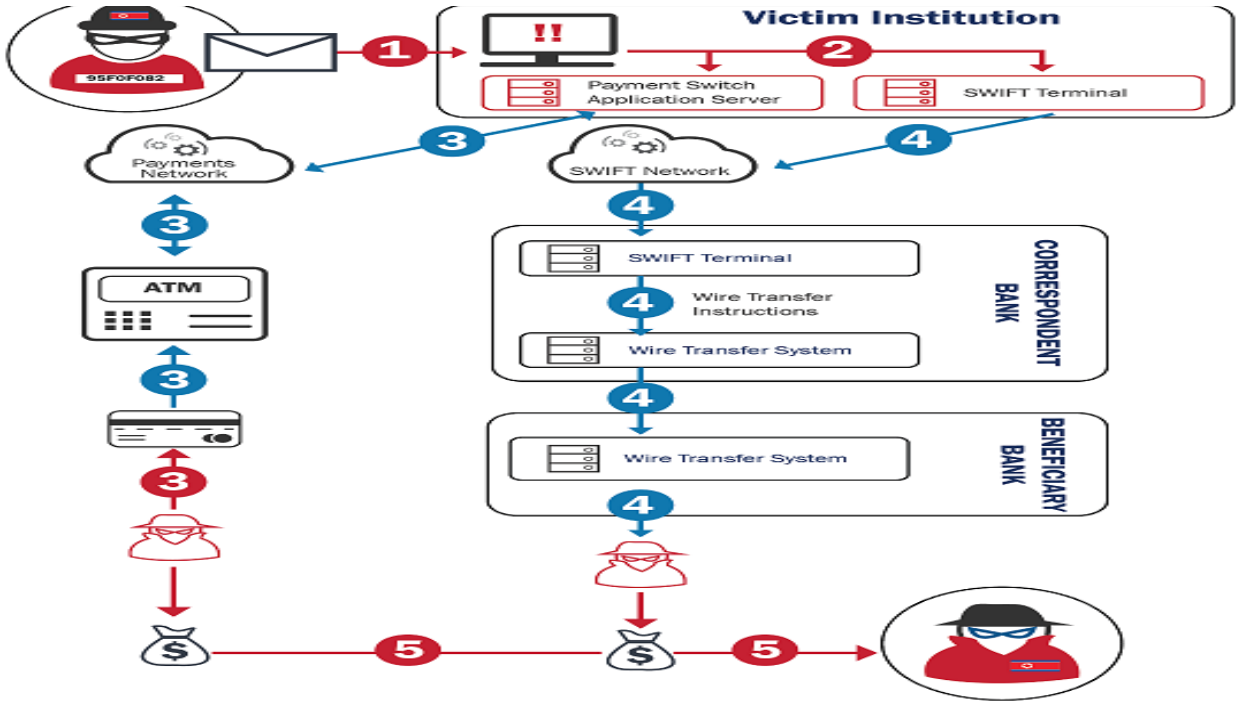
SUMMARY

A threat from an Iran-based malicious cyber actor is targeting several industries mainly associated with information technology, government, healthcare, financial, insurance, media sectors and other U.S.-based networks.

The attacker conducts mass-scanning and uses tools, such as Nmap, to identify open ports. Once the open ports are identified, the threat actor exploits CVEs related to VPN infrastructure to gain initial access to a targeted network. This threat actor used these vulnerabilities to gain initial access to targeted networks and then maintained access within the successfully exploited networks for several months using multiple means of persistence.

There are notable means of detecting this threat actor such as attackers use FRPC over port 7557 and ngrok which may appear as TCP port 443 connections to external cloud-based infrastructure. Administrators and network defenders must be able to identify a potential compromise of their network and protect their organization from future attacks.

HOW IT WORKS



SECURITY RISK

This threat actor has the capability to deploy ransomware on victim networks.

RECOMMENDATION

- Keep software up to date;
- Use a multi-factor authentication for all accounts; and
- Secure network infrastructure.

MITIGATIONS

- Secure access to infrastructure devices;
- Segment and separate networks and functions;
- Limit unnecessary communications; and
- Validate integrity of hardware and software.

REFERENCE

- https://us-cert.cisa.gov/ncas/alerts/aa20-259a