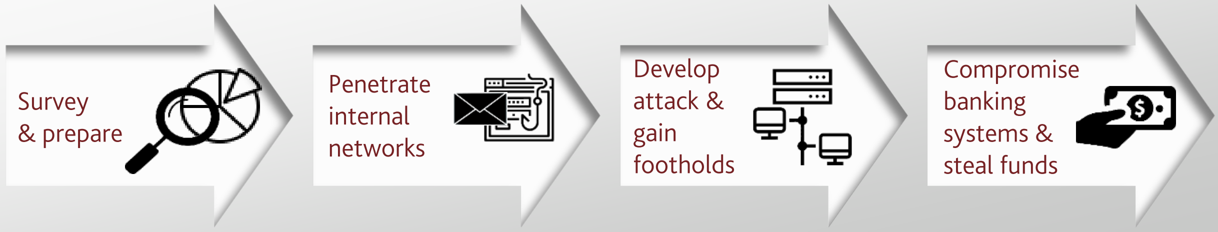
Bank robberies in the digital age

Despite the vast sums that the global finance industry spends on advanced security systems and innovations, financial crime continues to concern many across the sector. From phishing to counterfeit cheques, there are a number of crimes that must be on the minds of information security executive, not least digital bank robberies - robberies carried out on banks that can be carried out using computers, rather than the explosives and drills of classic Hollywood heists. The end result, though, is that criminals make off with a lot of money that have no right to - and that money is often used for nefarious purposes.

How do these attacks work?

Typically, intruders choose targets based on their technical expertise, available tools and knowledge of internal banking processes. The methodology is relatively straightforward:

Main attack stages



Survey & prepare
Penetrate internal networks
Develop attack & gain footholds
Compromise banking systems & steal funds

Main attack stages

Survey & prepare

This can be lengthy and time-consuming: attackers have to gather as much information about their target as possible. Since the use of external resources can be detected by security systems, criminals exploit passive methods to obtain information, such as identifying domain names and addresses belonging to the bank.

Penetrate internal networks

Once ready, the attacker systemically attempts to enter they target network from all external visible entry points using both technical and non-technical means. The attacker penetrates first layer of defence.

Proliferate the attack

Once criminals have gained access to the bank's intranet, they need to obtain local administrator privileges to continue their attack. Success relies on insufficient system protection against internal attackers. Common vulnerabilities include:

- Use of outdated software
- Failure to install OS security updates
- Configuration errors (including excessive user and software privileges, as well as setting local administrator passwords through group policies)
- Use of dictionary passwords by privileged users
- Absence of two-factor authentication

Compromise banking systems & steal funds

After gaining a foothold in the network, criminals need to understand where the target banking systems are and find the most convenient ways to access them. Criminals examine users' workstations in search of files indicating that a particular workstation has worked with bank applications.

Specialised software is usually used to store passwords for critical systems on corporate networks. An intruder with local administrator privileges can copy the memory dump of this process, extract passwords to access application or encrypted databases, and then obtain clear text passwords to all critical bank applications, including the core banking system, SWIFT and ATM management workstations.

Srikant Ranganathan
Senior Director
T +973 17206827
srikant.ranganathan@keypoint.com

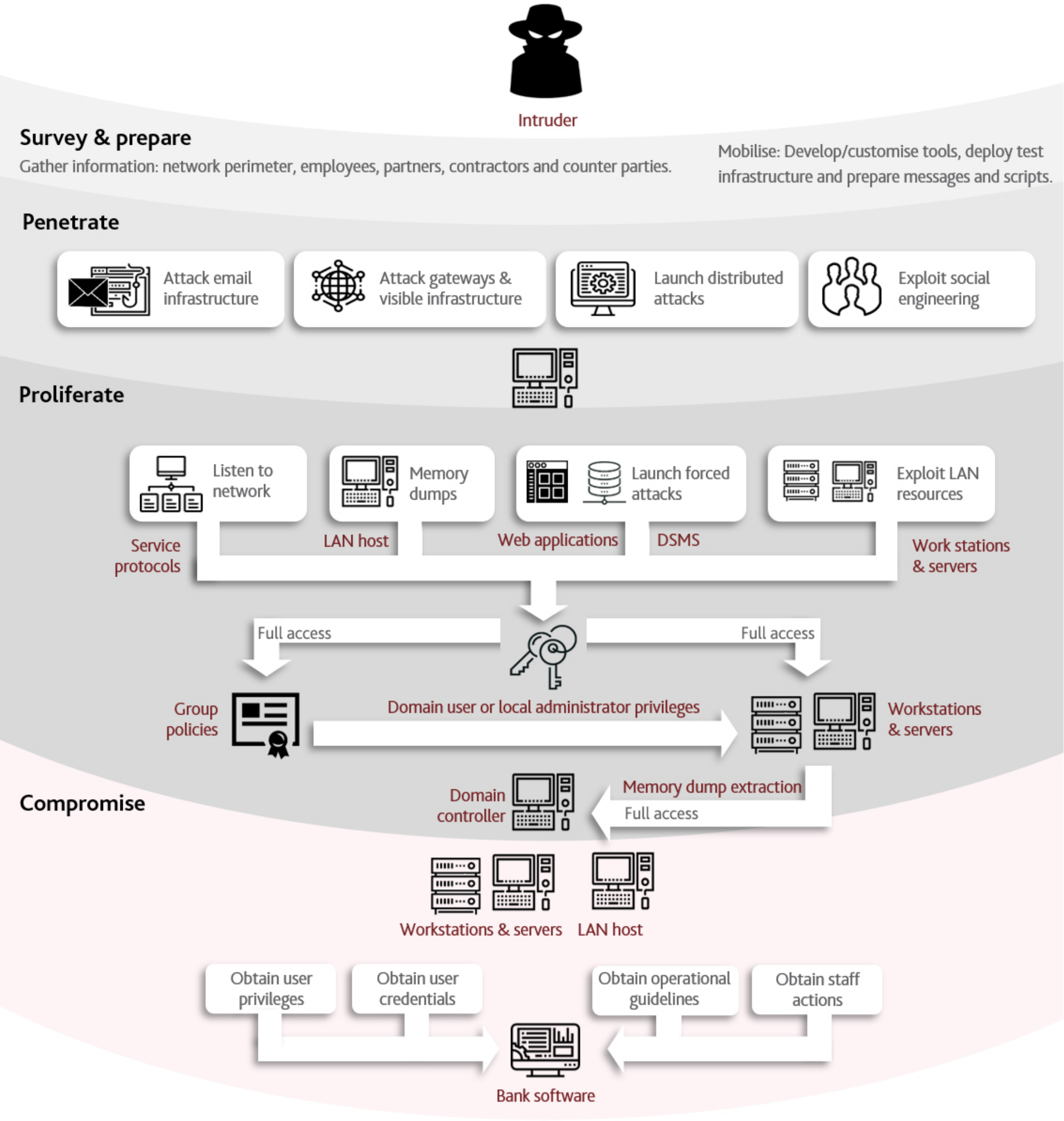
Sagar Rao
Assistant Manager
T +973 17206802
sagar.rao@keypoint.com

Embezzle funds

The main methods of theft include:

- Transferring funds to fictitious accounts through interbank payment systems
- Transferring funds to cryptocurrency wallets
- Controlling bank cards and accounts
- Controlling ATM cash dispensing

Financial crime continues to pose a major threat to the region's financial services industry. While the industry remains committed to tackling all of its many different forms, eradicating the threat - including digital bank robberies - requires the combined efforts of not just the banks themselves but also industry bodies, regulators and professional services companies like Keypoint.



Intruder

Survey & prepare

Gather information: network perimeter, employees, partners, contractors and counter parties.

Mobilise: Develop/customise tools, deploy test infrastructure and prepare messages and scripts.

Penetrate

Attack email infrastructure
Attack gateways & visible infrastructure
Launch distributed attacks
Exploit social engineering

Proliferate

Compromise

Embezzle funds