The GozNym criminal network: How it worked

1 SOURCING THE MALWARE

The **leader** of the criminal network (from Tbilisi, Georgia) leased access to the malware from a developer.

The developer (from Orenburg, Russia) worked with coders to create GozNym, a sophisticated piece of malware to steal online banking credentials from victims' computers.

2 RECRUITING ACCOMPLICES

The leader recruited other cybercriminals with specialised skills and services which they advertised on underground, Russian-speaking online criminal forums.

3 COVERING THEIR TRACKS

The leader and his technical assistant (from Kazakhstan) worked with 'crypters' (including one in Balti, Moldova) to crypt the malware so antivirus software would not detect it on the victims' computers.

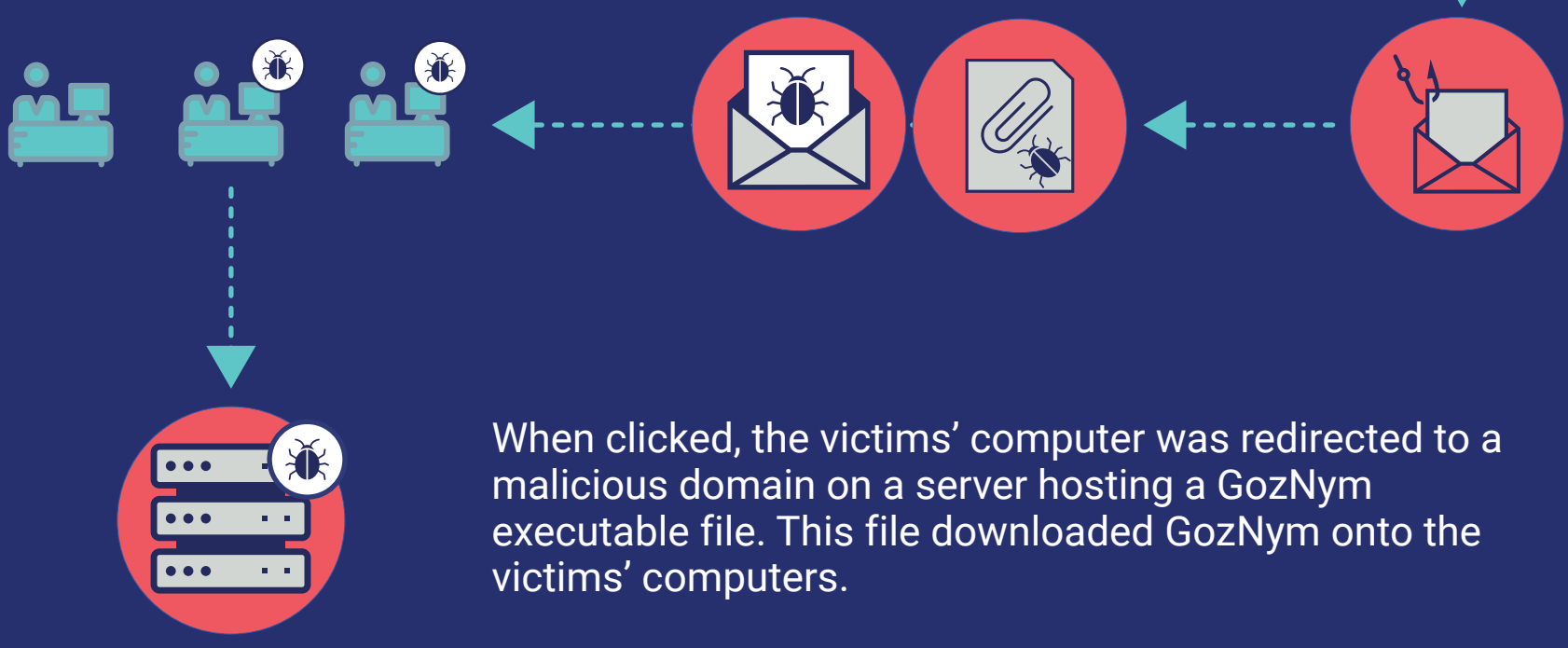
Crypters

4 DISTRIBUTION AND INFECTION

Spammers (including one in Moscow, Russia) sent phishing emails to hundreds of thousands of potential victims.

Spammers

The emails were designed to appear as legitimate business emails and contained a malicious link or attachment.

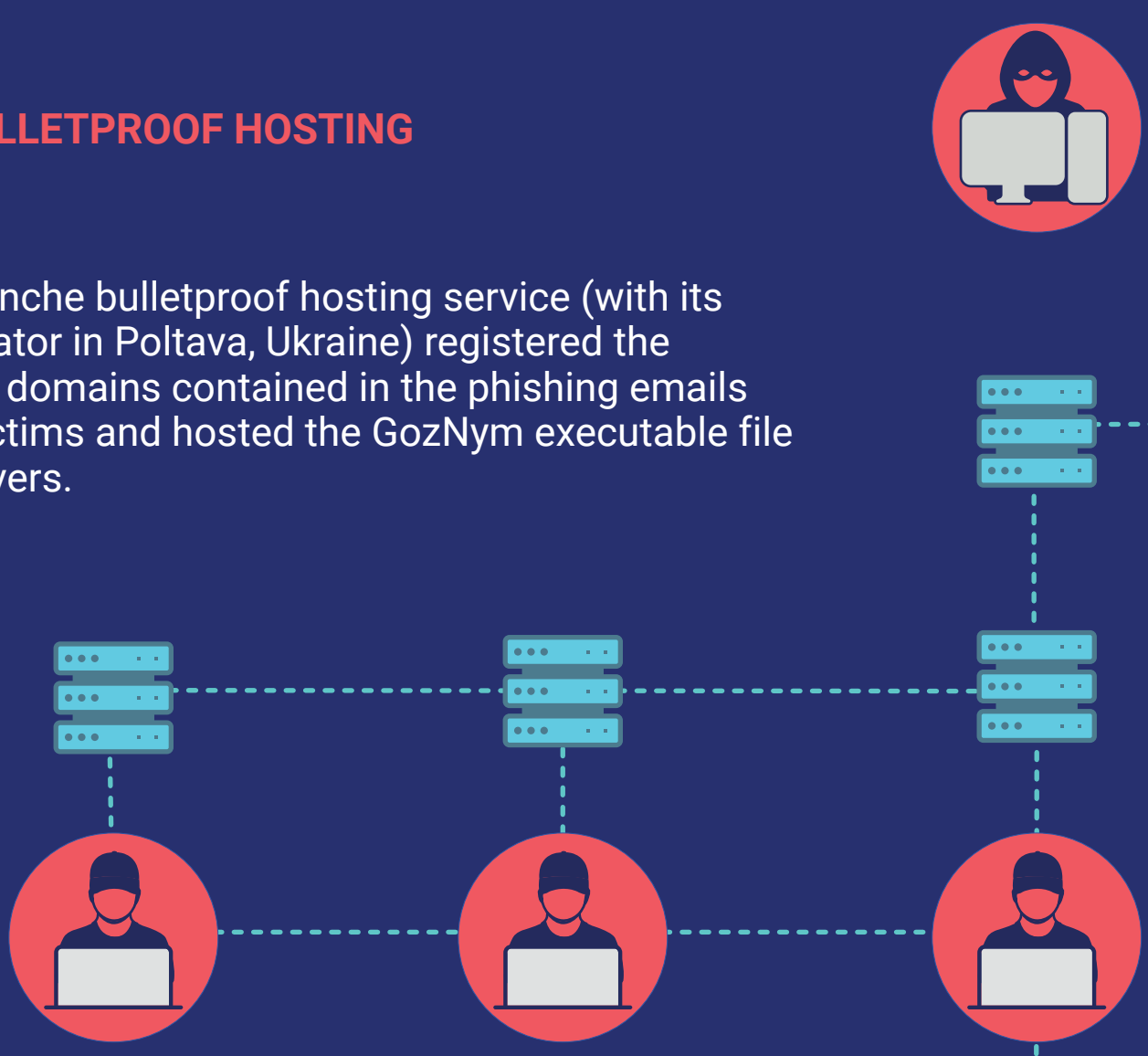


When clicked, the victims' computer was redirected to a malicious domain on a server hosting a GozNym executable file. This file downloaded GozNym onto the victims' computers.

The GozNym criminal network: How it worked

5 BULLETPROOF HOSTING

The Avalanche bulletproof hosting service (with its administrator in Poltava, Ukraine) registered the malicious domains contained in the phishing emails sent to victims and hosted the GozNym executable file on its servers.



Once infected, sensitive information from victims' computers was passed to the GozNym conspirators through a complex layer of servers designed to prevent detection by law enforcement and cybersecurity experts.

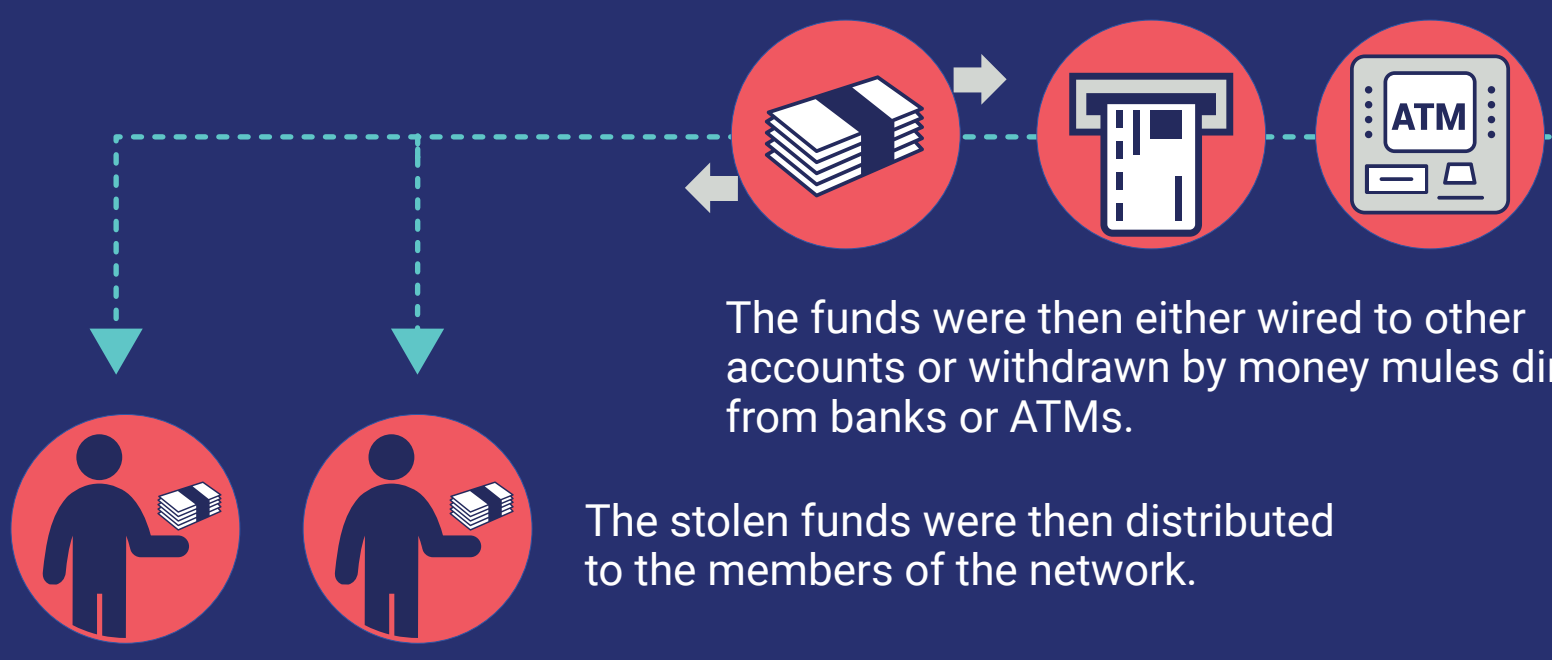
After GozNym stole victims' online banking information, it was sent to a central access panel.

6 TAKING CONTROL OF ACCOUNTS

Account takeover specialists (including one in Varna, Bulgaria) and a second in Khmelnytskyi, Ukraine (originally from Kazan, Russia), accessed the panel to gain unauthorised access to victims' online bank accounts from which they initiated electronic transfers of funds.

7 CASHING OUT

Sophisticated money launderers, known as cash-outs or drop masters, (including those in Stavropol, Russia; Volograd, Russia; and Nikolaev, Ukraine) provided bank accounts to receive victims' stolen funds.



The funds were then either wired to other accounts or withdrawn by money mules directly from banks or ATMs.

The stolen funds were then distributed to the members of the network.

The GozNym criminal network: How it worked

★ Leader ▼ Technical assistant ⬢ Hosting administrator ● Spammers

▲ Crypters or account takeover specialists ■ Cash-outs/drop masters

COOPERATION BETWEEN

Bulgaria Germany Georgia Moldova Ukraine

United States EUROJUST EUROPOL