MWR INFOSECURITY

Supported by CPNI Centre for the Protection of National Infrastructure

CASE STUDY:

Attack Type – Phishing with Malware

Scenario:

Org 10 is a large multi-national financial services provider. Org 10 began receiving notifications from various customers regarding phishing emails that appeared to originate from its mail server and resulted in customer's computer systems becoming infected and their customers losing their money through fraud. The phishing emails contained an attachment that was identified as a malicious trojan by antivirus (AV) software running on some of the customer systems. Org5 initiated an investigation.

The emails were examined and, although they looked and felt like an email from Org 10, examination of the mail headers showed that they were an imitation that had been sent from a compromised third party mail server. Targeting of Org 10's customers is believed to have occurred as the result of a web application vulnerability on their website that allowed attackers to derive all of their customer's email addresses.

The email attachment was a file named "Statement_Jan_2015.zip". The zip file contained a malicious executable named "Statement_Jan_2015.exe". The email evoked emotion as a distraction by claiming to report a large overdraft on the owner's account.

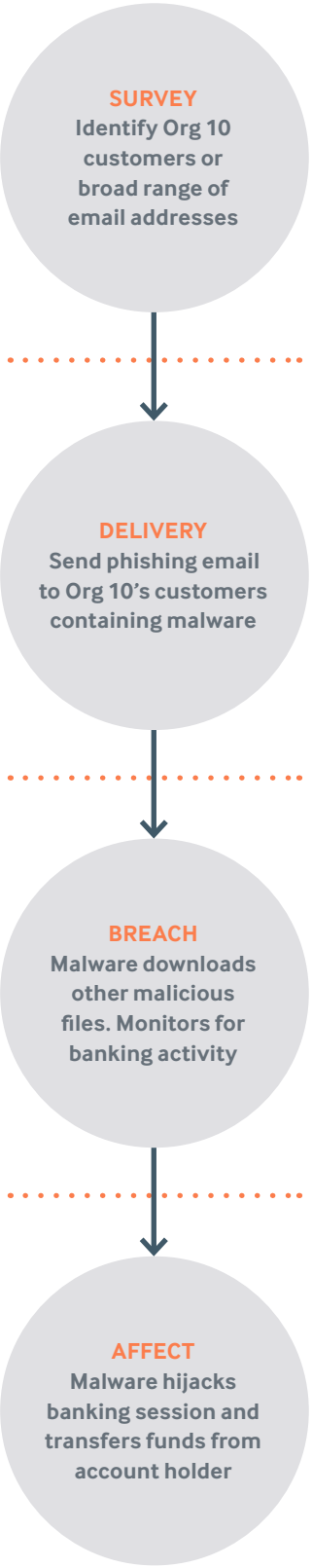
The attached malware was consistent with the Zeus family of Trojans and had the ability to steal personal data from affected systems. The type of collected data can include banking information, login credentials, or any other information of interest to the attacker. Once installed on the infected system, the malware connects to command and control servers or malicious sites to download additional malware, and upload collected data.

The malware gained persistence on the infected machines and extracted personal data as well as initiating transfers from the user's bank accounts to accounts controlled by the malware authors. Org 10 found that, although anti-virus products update regularly to detect the malware variants, the authors change the malware so often that their customers continue to become re-infected on a regular basis.

Specific Failures Leading to Compromise

- Web application vulnerability allowing usernames to be derived
- Insufficient communication with customers indicating that attachments are never sent

STAGES OF ATTACK



ATTACK TIMELINE

Targeting to Compromise:	Hours (dependant on opening and executing email)
Compromise to Exfiltration:	1 Day
Compromise to Discovery:	1 Day
Compromise to Containment:	10 Days
Method of Discovery:	External – Customer identified that money has left their account
Threat Actor:	External – targeted
Assets Compromised:	End User System, Org 10 Financial customer authentication credentials
Business Impact:	Medium – customers defrauded which Org5 had to recompense for