Title: Customer Security Issues Update – New information

Dear SWIFT User

New malware identified in bank's environment. No impact on SWIFT network, core messaging services or software.

As we notified you in our earlier communications, we are aware of a small number of recent cases of fraud at customer firms. First and foremost we would like to reassure you again that the SWIFT network, core messaging services and software have not been compromised. We have however now learnt more about a second instance in which malware was used – again directed at banks' secondary controls, but which in this instance targets a PDF Reader used by the customer to check its statement messages.

Forensic experts believe this new discovery evidences that the malware used in the earlier reported customer incident was not a single occurrence, but part of a wider and highly adaptive campaign targeting banks.

In both instances, the attackers have exploited vulnerabilities in banks funds' transfer initiation environments, prior to messages being sent over SWIFT. The attackers have been able to bypass whatever primary risk controls the victims have in place, thereby being able to initiate the irrevocable funds transfer process. In a second step, they have found ways to tamper with the statements and confirmations that banks would sometimes use as secondary controls, thereby delaying the victims' ability to recognise the fraud.

The attackers clearly exhibit a deep and sophisticated knowledge of specific operational controls within the targeted banks – knowledge that may have been gained from malicious insiders or cyber attacks, or a combination of both.

Preventative Controls

As a matter of urgency we remind all customers again to urgently review controls in their payments environments, to *all* their messaging, payments and ebanking channels. This includes everything from employee checks to password protection to cyber defences. We recommend that customers consider third party assurance reviews and, where necessary, ask your correspondent banks and service bureaux to work with you on enhanced arrangements.

We also urge all customers to be forthcoming when these issues occur so that the fraudsters can be tracked by the authorities, and SWIFT can inform the rest of community about any findings that may have a bearing on wider security issues.

In the meantime we would like to reassure you that the SWIFT network, SWIFT messaging systems and software have not been compromised. The security and integrity of our messaging services are not in question as a result of the incidents. We will continue with our security awareness campaign, bilaterally with users and through industry forums and other appropriate channels. We will also continue working with our overseers, with law enforcement agencies, and third party experts, and we will continue to inform you of any further information we believe that can help you detect or avert such attacks.

Latest Findings

In the earlier case we reported to you, and this particular case we can confirm that: malicious insiders or external attackers have managed to submit SWIFT messages from financial institutions' back-offices, PCs or workstations connected to their local interface to the SWIFT network. The modus operandi of the attackers is similar in both cases:

1. Attackers compromise the bank's environment
2. Attackers obtain valid operator credentials that have the authority to create, approve and submit SWIFT messages from customers' back-offices or from their local interfaces to the SWIFT network.
3. Attackers submit fraudulent messages by impersonating the operators from whom they stole the credentials.
4. Attackers hide evidence by removing some of the traces of the fraudulent messages.

In this new case we have now learnt that a piece of malware was used to target the PDF reader application used by the customer to read user generated PDF reports of payment confirmations. The main purpose of the malware is again to manipulate an affected customer's local records of SWIFT messages – i.e. step 4 in the above modus operandi.

Once installed on an infected local machine, the Trojan PDF reader gains an icon and file description that matches legitimate software. When opening PDF files containing local reports of customer specific SWIFT confirmation messages, the Trojan will manipulate the PDF reports to remove traces of the fraudulent instructions.

There is no evidence that the malware creates or injects new messages or alters the content of legitimate outgoing messages. This malware only targets the PDF reader in affected institutions' local environments and has no impact on SWIFT's network, interface software or core messaging services.

Customers that use PDF reader applications to check their confirmation messages should take particular care.

For an indicator of compromise (IOC) that allows you to learn more technical details and help to verify whether your operating environment is affected by the abovementioned malware affecting the PDF reader, please consult KB tip XXXXXXX.

Your Security

As we stated earlier, this is clearly a highly adaptive campaign targeting banks' payment endpoints. Above all therefore your first priority should be to ensure that you have all preventative and detective measures in place to secure your environment. This latest evidence adds further urgency to this work. Such measures are the best defence against such malware being installed on your local systems, and against fraudulent actions on your local infrastructure to connect to the SWIFT network.

Please remember that as a SWIFT user you are responsible for the security of your own systems interfacing with the SWIFT network and your related environment – starting with basic password protection practices – in much the same way as you are responsible for your other security considerations. Whilst we issue, and have recently reminded you about, security best practice recommendations, these are just a baseline and general advice.

We will continue to update you on these issues as more information becomes available to us. We would ask you to ensure that these communications reach your security officers.

Yours faithfully

SWIFT

For further information, as well as SWIFT's security guidance covering a number of different interface solutions, please consult the Knowledge Base tip 5020786 on SWIFT.com.