



IdenTrust™ Fraud Alert

FBI warns of Significant Fraud Increase due to “Zeus” Malware

What is Zeus?

Zeus is a highly sophisticated and malicious Trojan horse computer program. It has infected tens of thousands of machines around the world, resulting in multimillion dollar fraud losses. Zeus is, the latest and greatest in a long line of increasingly sophisticated malware targeted at Internet banking, and should be a concern to banks and their customers everywhere.

The Trojan compromises the safeguards banks have put in place to allow customers to access their online services, such as one-time-password generators. Zeus steals the details of the security safety guards and stores them on a remote server. This information in combination with other techniques, such as controlling the web pages a user sees (believing they are interacting with a legitimate web site) allows criminals to defraud account holders without their knowledge.

Some banks have reacted by introducing additional ‘out-of-band’ counter-measures, such as calling the customer to confirm their transaction or the use of geo-locators, but the fraudsters have also compromised these security actions.

The FBI has stated that the threat stems not only from the malware involved, but also the lack of controls at financial institutions and 3rd party providers. For example “Zeus” is currently detected only 23% of the time by antivirus applications, according to Trusteer researchers.

The Internet Crime Complaint Center (IC3), a partnership between the FBI, the National White Collar Crime Center and the Bureau of Justice Assistance, issued a November alert, calling attention to the rapidly increasing number of attacks and highlighting the areas that are most vulnerable. In most cases the attacks take place through fraudulent use of ACH and other EFT networks, targeting small to medium sized businesses. In November cyber thieves sent out millions of emails impersonating NACHA, complaining about an unauthorized, rejected or failed ACH transaction. The threat is global, as evidenced by the attack on 20 European Banks in recent months.

How Zeus Works

In most instances, the attacks begin with a “phishing” email that contains an infected file or a link to a malicious website. The target of the email is generally a company official or employee with the ability to initiate funds transfers. Once the malware is activated, the malware triggers a keylogger that harvests banking credentials, which are then used either from another computer or in a hidden virtual session on the individual’s computer. ACH transactions are initiated and the funds are sent to “money mules” who then transfer them to overseas accounts.

The IdenTrust Solution – Trust Gate

IdenTrust multi layered security systems provide protection from Man-in-the-Middle (MITM) and Man-in-the-Browser (MITB) threats. IdenTrust Trust Gate is a hardened USB device containing all of the necessary components to create a digital signature and execute two-factor authentication. Trust Gate is a zero footprint solution; users can plug it in to any workstation with Internet connectivity and access applications securely. Users and customer support staff are liberated from installation, compatibility concerns, privilege management, and other obstacles traditionally associated with hardware based solutions. In essence, Trust Gate delivers greater security than traditional PKI solutions and is easier to use than the far less secure One Time Password device.

Trust Gate Benefits

Security

- Full anti-Phishing protection
- Defense against all known fraud exposures, such as Man-in-the-Middle, Man-in-the-Browser and sophisticated malware including Zeus
- Multiple layers of protection including defense against key loggers at the operating system level and a secure browser with locked-down configuration which negates the threat of malicious software infection
- High assurance login mechanism using digital signatures – applications can verify the integrity of the transaction cryptographically and check status of the certificate in real-time
- Stronger authentication than One Time Passwords (OTP’s)

User Experience

- Completely portable – no need to install any client software enabling the token to be used with any PC anywhere
- Remote and highly secure token software update mechanism – token software can be updated in real-time. No need to reissue hardware to combat new exposures
- You only need one – one token for any bank application, in any country and for use across any network