

Gozi Trojan - king of evasion continues to avoid sophisticated detection

- *TrustDefender Labs analysis shows increasing threats of Trojans*

4th November 2010: The recent TrustDefender Labs report has alarmingly discovered another variant of the Gozi Trojan with a 0% detection rate. TrustDefender Labs has recently re-analysed the Trojan Gozi, (pronounced goh'-zee), which has been showing fraudulent attacks since 2007. Their research highlights how the Gozi Trojan is very professional, efficient and attacks financial institutions worldwide by managing to stay under the radar and remain undetectable. By targeting specific financial institutions (mainly business and corporate banking in the US) Gozi endeavours not to attract industry attention with this approach. While everybody is talking about Zeus, Gozi can do its dirty work.

During the TrustDefender Labs tests the Gozi Trojan was invisible to all leading anti-virus software, allowing it to infiltrate and attack user's systems and browsers. The new Gozi variant has many of the same characteristics of its predecessor (researched 12 months ago) however, is showing increasing sophistication in HTML injection compared to other Trojans. Gozi perpetrators have been successfully evading signature patterns so consistently that the evolution of the Trojan has been relatively unknown. This highlights the potential risks and impacts of attacks on financial institutions, businesses and individuals whilst staying predominantly undetectable to any anti-virus software.

Online Security expert and CTO of TrustDefender, Andreas Baumhof comments; "Gozi is unbelievably good at staying under the radar from an infection point of view, but this particular sample also used SSL and HTTPS against the good guys. Typically designed to protect us, the fraudulent use of HTTPS helps them to stay virtually invisible for their C&C server connection. Alarmingly we are coming across an increasing number of Trojans that are using SSL and HTTPS to cover their tracks. The other thing that impressed us was the extensive client-side logic to circumvent even Two-Factor Authentication. Unfortunately this is becoming more common as we see similar techniques with Trojans such as Zeus, Spyeye, Carberp."

Why should we be worried about Gozi?

- Gozi is one of the most sophisticated Trojans out there with an impressive feature set.
- Gozi can use encrypted HTTPS connection for its C&C server communication with a valid certificate meaning it can evade detection.
- Traditional anti-virus software is unable to detect the Gozi Trojan
- Gozi features an extensive client side logic (in JavaScript) to be able to work with many different banking websites and also allowing it to steal static information (such as maiden name) and also dynamic password schemes (such as Two-Factor Authentication and One-Time-Passwords). This is similar to Zeus, Spyeye, Carberp and Silon
- Gozi enables real time account takeover that even works with Two-Factor Authentication.

ENDS

For more information visit:

www.trustdefender.com and www.trustdefender.com/blog

For any further media information or an interview contact:

Sharon Ghatora or Monique Jones Taurus Marketing

Phone: +61 2 9415 4528 or +61 416 890 648 / +61 413 689 343

Email: sharon.ghatora@taurusmarketing.com.au / monique@taurusmarketing.com.au



TrustDefender will fully detect and protect against Gozi. The TrustDefender online transaction security solution was designed to protect the user and the financial institution right from the start.

TrustDefender explained:

- TrustDefender solves the issues facing financial institutions where an increasing percentage of their customer base connects to online banking services with malware infected computers.
- Furthermore financial institutions have no visibility in real-time to see whether their customers have taken care of their computers and therefore the enterprise cannot distinguish between an infected or clean computer. This leaves the financial institution and the user at risk.
- TrustDefender's unique technology, evaluates the security health risk of a computing device, allowing the business to detect the ever increasing sophistication of malware, immediately act and stop a potential threat through the application of business rules and policies in real-time before any authentication process begins;
- TrustDefender provides key information to online enterprises including financial institutions, while giving the enterprise risk manager a real-time risk profile of the endpoint computers access their website.
- TrustDefender can be easily integrated with existing and older risk management engines to enhance the capabilities of these technologies.
- TrustDefender provides the enterprise with the ability to not only protect the customer but also notify the customer of any security threats and advise them how to deal with any potential risk. The Safe&Secure Mode will make sure a customer can always securely login and fix the problem at a later date.

About TrustDefender

TrustDefender is the worldwide leading provider of 'real-time risk based online transaction security solutions' to safeguard consumer, financial institution and business online transactions. TrustDefender's revolutionary technologies enable users to verify its security health state, perform a memory forensics analysis and secure their mobile computing device in real-time - before and during any Internet transactions.

At the same time, TrustDefender provides real time feedback on the security health of their computer. Best yet, the user does not need to be a security expert to use this technology. Most importantly, for the first time, the financial institution has real-time information that they can use to better protect transactions from compromise and also allows the enterprise risk managers to finally get a real time risk profile of their customer base.

The Enterprise Server incorporates a real-time risk-scoring engine that together with the rules and policy engine is always in control and can give the financial institution a server-side tool to mitigate the risk on both ends and includes an extensive Auditing and Reporting module. TrustDefender is the world's first security solution which enables online businesses to integrate the home user or end user's PC into one overall security chain.

TrustDefender was founded in December 2005 after the founders discovered the traditional security model was broken – and decided to fix it.