Issued 4/5/17

Custom Phishing Attacks Grow as Crooks Create Fake Flight Confirmations, Receipts

Cyberattackers are carefully crafting individual phishing emails purporting to be from airlines and financial departments to deliver malware -- and they're even mimicking internal corporate travel and expenses systems to steal personal details from the victims they target.

While cybercriminals using the lure of fake travel itineraries to dupe staff working in sectors reliant on shipping goods or employee travel isn't new, researchers have uncovered a particularly advanced phishing attack. Discovered by cybersecurity researchers at Barracuda Networks, this airline phishing attack uses a variety of techniques to capture sensitive data from victims and deploy an advanced persistent threat.
The email from the attacker impersonates a travel agency or an employee in the target's own HR or finance department. The email's subject line claims it's a forwarded message about a flight confirmation, stating the airline, the destination, and the price of the flight.

Once opened, the email presents the target with an attachment in the form of a PDF or Microsoft Word document. The attachment purports to be a flight confirmation or receipt but, of course, it's neither of these things. When the target opens the attachment, the malware runs immediately, dropping an advanced persistent threat into the network, and enabling the

attacker to stealthily monitor the infected organisation -- likely with the aim conducting espionage and stealing data.

Another variant of this attack which, instead of dropping malware to stealthily steal data, uses phishing links to directly take sensitive information from the victim. In these instances, the phishing website is designed to look like an airline website or even the expenses and travel system used by the target's company.

These phishing links are ultimately designed to trick the victim into supplying sensitive corporate credentials, which the attackers will then use to infiltrate the company network, databases, and emails in order to steal information.