Abstract
The financial services industry once again finds itself under cyber-attack, this time the victim of their own digital tellers. In recent weeks, banks in Russia, United Kingdom, Taiwan and other countries have suffered from mega breaches originated in compromised ATMs. Hackers are setting their sights on the massive holiday season trade volumes hoping to disrupt the financial services industry. While new authentication standards such as chip-equipped cards, PINs and geo-blocking are helping to prevent card-based fraud, malware targeting point of sale systems and ATMs continue to evolve at an exponential rate.

The High Cost of ATM Hacks
In June, ATM's produced by Wincor Nixdorf and operated by Taiwan's First Bank[i] suffered a massive breach as hackers used connected devices and self-deleting malware to force the machines into spitting out nearly $2 million dollars. A bank in South Africa was robbed of $13 million dollars when hackers used fake credit cards to withdraw money from ATMs in Japan[ii]. The State Bank of India[iii] blocked and reissued bank cards after malware was discovered on non-SBI ATM's. Hackers frequently use ATM skimmers or DIP readers - card readers that work by the user inserting their card (versus swiping).

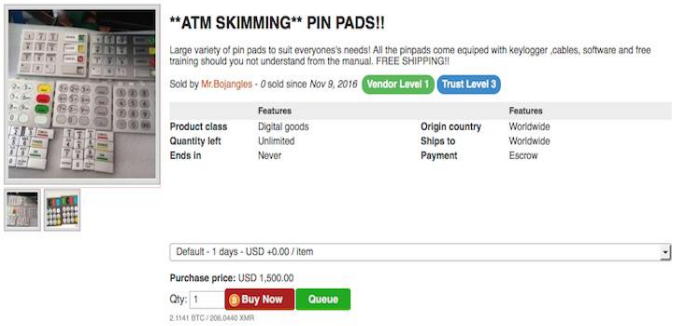

Figure 1: ATM Skimmer for sale on AlphaBay

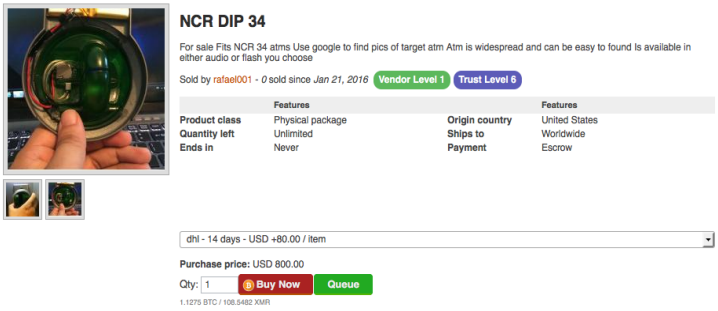

Figure 2: NCR DIP 34 for sale on AlphaBay - a false cover containing card skimmer components

Tesco £2.5 Million Loss
On November 5, UK Tesco Bank suffered a breach that resulted in 9000 accounts being compromised and £2.5 million[iv] were stolen from customer accounts. Tesco customers began to notice suspicious activity and withdrawals from their accounts that prompted Tesco to **suspended online debit transactions** as a precautionary measure.

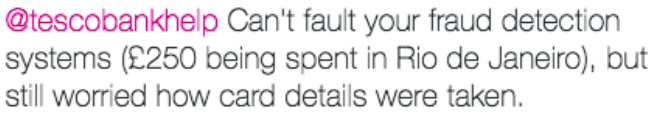

Figure 3: Example of Tesco Bank breach and customer's reaction`

While Tesco Bank is conducting their investigation, there are a number of possibilities. Some claim the attack targeted contactless payments or the Tesco mobile app while others claim it was an inside job. Two months ago, Europol issued an alert stating that cyber criminals have begun targeting Android phones to trigger fraudulent tap-and-go, NFC payments from software that allows criminals the ability to upload compromised cards to their phone. Darknet users are discussing how easy it is to cash out Tesco accounts and reference an insider at the bank.

Figure 4: An Alphabay member references Tesco Insider

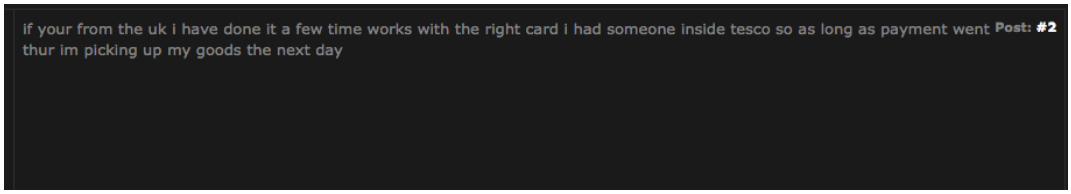

Figure 5: 2015 Tesco insider referenced

Russian Banks

Following the Tesco attack – but not related - on November 8th, five banks in Russia experienced a DDoS attack from what some are reporting[v] as a DDoS-for-hire attack originating from the darknet marketplace, AlphaBay. The botnet – claimed by the vendor to be based on IoT devices – offered a variety of attack vectors, as well as high bursts of traffic volumes. The target list included Sberbank, Alfabank, Bank of Moscow, Rosbank and the Moscow Exchange. This attack lasted for two days, disrupting service operation for several hours.

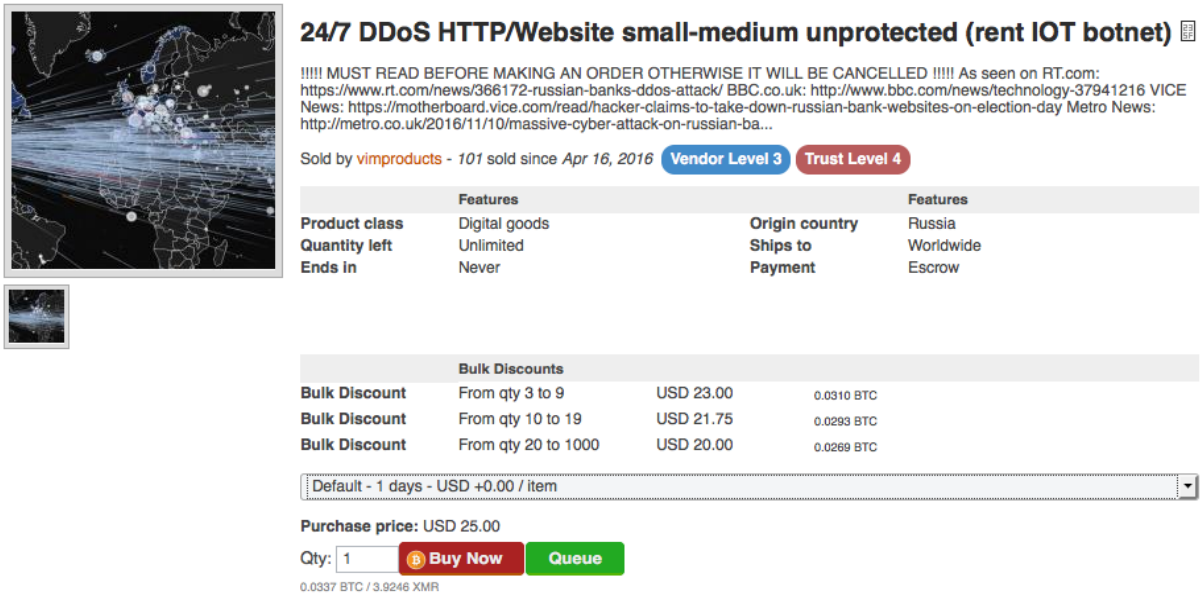

Figure 6: DDoS for hire on AlphaBay

More November Attacks Against Banks

Following the attacks against Russian banks, political hacktivists began launching Cross-site-scripting and LFI attacks against JPMorgan Chase, Barclay Bank, and the Royal Bank of Scotland.

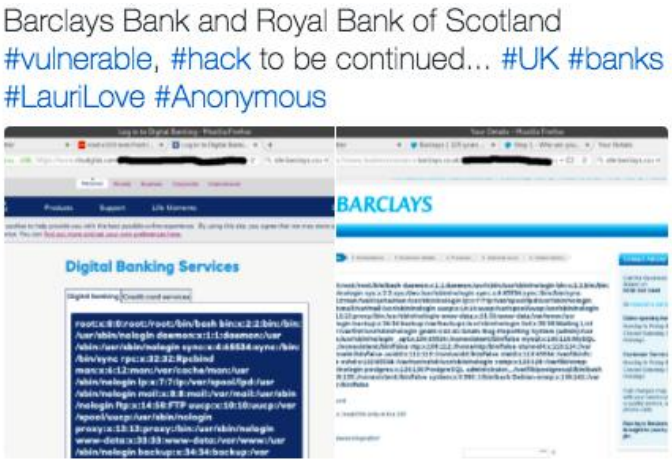

Figure 7: LFI vulnerability in Barclay and Royal Bank of Scotland website

Hackers have different ways to leverage stolen data on the darknet:

- Sell it themselves (card numbers, PIN codes etc.) in bulks or individually.
- Share profit with a middlemen willing to cash-out the accounts.
- Upload these compromised accounts onto mobile wallets and cash them out in local stores.

Hacking Web Application Techniques

Cross-site Scripting - In this attack, malicious scripts are injected into websites through a web application flaw where there is no validation of user input used by the application

SQL Injection - This technique takes advantage of poor application coding. When the application inputs are not sanitized it becomes vulnerable. Attackers can modify an application SQL query to gain access to unauthorized data with administrator access, run remote commands on the server, drop or create objects in the database, and more.

Remote File Inclusion (RFI) - This is a type of vulnerability most often found on PHP running websites. It allows an attacker to include a remotely hosted file, usually through a script on the web server. The vulnerability occurs due to the use of user-supplied input without proper validation. This can lead to something as minimal as outputting the contents of the file, but depending on the severity can lead to arbitrary code execution.

Local File Inclusion (LFI) – This is very much like RFI; the only difference is that in LFI the attacker has to upload the malicious script to the target server to be executed locally.

DDoS as a Service

For a small fee, botnet owners provide access to leverage their network for the purpose of launching Distributed-Denial-of-Service attacks for profit. DDoSaaS, AKA booters or stressers offer a web-based attack service that provides users with a user-friendly interface and various attack vectors to leverage. Vendors also sell slots or access to these botnets via darknet marketplaces. Prices range between $19.99 to over $1000 dollars depending on the attack duration, sophistication and volume.

Web Application Security Considerations for Organizations Under Threat

- **Full coverage** of OWASP Top-10 application vulnerabilities
- **Low false positive rate –** combining negative and positive security models for maximum accuracy
- **Auto policy generation** capabilities for the widest coverage with the lowest operational effort.
- **IP-agnostic device fingerprinting** capabilities to overcome dynamic IP attacks and achieving improved bot detection and blocking
- **Flexible deployment options -** on-premise, out-of-path, virtual or cloud-based

DDoS Protection Considerations for Organizations Under Threat

- Hybrid DDoS Protection - (on-premise + cloud) – for real-time protection that also addresses high volume attacks and protects from pipe saturation.
- Behavioral-Based Detection - to quickly and accurately identify and block anomalies while allowing legitimate traffic through.
- Real-Time Signature Creation - to promptly protect from unknown threats and 0-day attacks.
- A cyber-security emergency response plan - that includes a dedicated emergency team of experts.

Radware urges companies to inspect and patch their network in order to defend against risks and threats.

Under Attack and in Need of Expert Emergency Assistance? Radware Can Help.

Radware offers a service to help respond to security emergencies, neutralize the risk and better safeguard operations before irreparable damages occur. If you're under DDoS attack or malware outbreak and in need of emergency assistance, Contact us with the code "Red Button".

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.

---

[i] http://money.cnn.com/2016/07/14/news/bank-atm-heist-taiwan/
[ii] http://money.cnn.com/2016/05/23/news/bank-fraud-south-africa-japan/index.html?iid=EL
[iii] https://www.hackread.com/atm-malware-hack-state-bank-of-india/
[iv] https://www.digitalshadows.com/blog-and-research/leak-on-aisle-12-an-analysis-of-competing-hypotheses-for-the-tesco-bank-incident/
[v] http://motherboard.vice.com/read/hacker-claims-to-take-down-russian-bank-websites-on-election-day