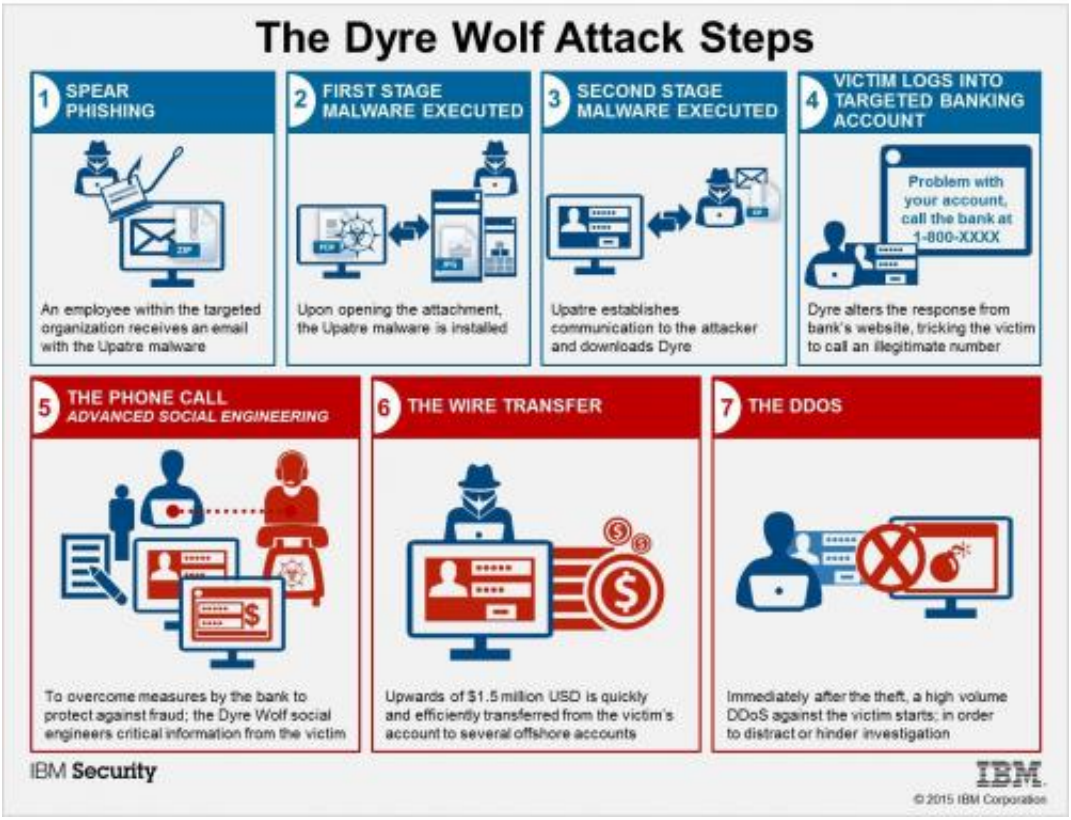
# Corporate accounts targeted in Dyre Wolf campaign

April 5 2015, by Nancy Owano




Credit: IBM

A sophisticated and brazen theft operation has been brought to attention this month by IBM Security, which refers to it as the "Dyre Wolf Campaign." It has been active and successful, having stolen over $1 million from targeted enterprise organizations. Victim organizations

have thus far lost between $500,000 and $1.5 million to the attackers. IBM Managed Security Services' John Kuhn, a senior threat researcher, recently delivered a detailed account of its roots and tactics used.

The campaign is siphoning off big bucks and seems hungry for more. The present-day thieves use a variant of the Dyre malware. Last year, IBM's Ori Bach, a risk management expert, had reported on the Dyre Trojan against major brand-name banks. Users were tricked into answering authentication challenges through fake websites eluding risk engines. By October last year, the IBM Trusteer team reported an infection rate increase of Dyre malware, from 500 instances to nearly 3,500. It was clear that Dyre was going after organizations, not individuals, for their big payouts.

Fast-forward to April 2015. The attackers are targeting organizations that frequently conduct wire transfers with large sums of money. Kuhn said, "social engineering and the resulting banking credentials theft is the focus of this new campaign and is ultimately what is used to illicitly transfer money from victims' accounts."

How the malware operators do it: They have created a process that involves (1) phishing (2) malware and (3) phone calls. These attackers rely on the fact that some employee, despite general cautionary statements in the news and in handbooks to stay away from links from unknown sources, is going to open a suspicious email and unsafe attachments; the infection adventure begins. Once opened, the victim is infected with the Upatre malware, which is a malicious code used as downloader for the Dyre agent, said the blog, *Security Affairs*.

*Ars Technica*'s security editor Dan Goodin said infected machines send out mass e-mails to other people in the victim's address book. "Then the malware lies in wait." A business employee on an infected computer tries to log into a bank website; Dyre is programmed to monitor the site

and the employee sees a new screen, not the real bank site, which says the site has issues and the employee needs to call a number for help in logging in.

The employee makes the call and provides the banking credentials the criminals need. (Bill Rigby, Reuters correspondent, said, "If users call that number, they get through to an English-speaking operator who already knows what bank the users think they are contacting. The operator then elicits the users' banking details.") Michael Mimoso in *Threatpost* said the U.S.-based victims told IBM that the scammers spoke "perfect English."

The wire transfer happens with money bouncing from foreign bank to foreign bank. Mimoso noted the hackers conduct wire transfers to offshore accounts. One organization targeted with the campaign also experienced a DDoS, said Kuhn.. "IBM assumes this was to distract it from finding the wire transfer until it was too late."

*Threatpost* reported Kuhn's thoughts about their social engineering tactics. According to *Threatpost*, Kuhn said, "'It's new and very brazen to have a call center to social engineer passwords out of people."

Rigby said the IBM-discovered scheme was being run by a "well-funded Eastern European gang." Mimoso noted that Dyre comes pre-loaded with web injects for hundreds of banks. What is more, Dyre malware changes to avoid detection. The gang appears to have an engineering team who is quite capable of code revisions to get past perimeters with, in some instances, complete code rewrites, changing names, hash, compression style, attachment icons. Global infection rates continue to climb with most of the victims in North America, said Mimoso.

Among the recommendations from IBM Security was to "Consider conducting periodic mock-phishing exercises where employees receive

emails or attachments that simulate malicious behavior. Metrics can be captured on how many potential incidents would have happened had the exercise been a real attack. Use these findings as a way to discuss the growing security threats with employees."

**More information:** securityintelligence.com/dyre-wolf/#.VR-t4-6UfGO