Get wise about Dyre: next-generation malware

As banks and businesses develop more sophisticated ways to deter and defend against information security threats, the cybercriminals behind those threats are continually working to get one step ahead. The latest is a new malware variant called Dyre (AKA Dyre Wolf or Dyreza). This malware strain has been specifically crafted by cybercriminals to target the banking accounts of various companies, from small businesses to large corporations, in an effort to pilfer millions of dollars.

Evidence of Dyre started appearing on the radar of banks and security researchers toward the end of 2014, and infection rates and attacks leveraging Dyre have rapidly increased.

The infection

As with many other virus and malware variants, the attack starts with a focused set of phishing emails; also known as spear-phishing. In some instances, the criminals behind Dyre have targeted financial staff of organizations likely to process large wire transactions. Perpetrators sent these emails under the guise of several different financial and regulatory topics with subject lines such as “Important, FDIC restrictions will be applied,” “ACH transaction rejected,” or “Critical notice about your ACH transaction.” In some cases, these emails seem to come from customer service of a bank or organization, such as “customersupport@yourbankname.com” or “support@ nacha.org,” when in reality they are not. The email contains a malicious attachment or a link that contains a malicious file or script that, once opened, is meant to exploit weaknesses on the user’s computer and install malware.

Perpetrators are sending other non-financial related phishing emails related to Dyre as well, many of them referencing invoices or faxes with malicious attachments.

Tips for avoiding malware

1. *Inform your staff about current security threats. Stay vigilant and aware.*
2. *Teach staff to watch for and detect phishing emails. Don't click links or open attachments in unsolicited emails.*
3. *Perform phishing tests to measure the efficacy of staff awareness and training programs.*
4. *Don't ever give out your username, password or one-time password. Be suspicious if you see a pop-up message that the website is down when logging in or making payments.*
5. *Require a two-step approval approach to approve online payments.*

The attack

Once the malware has been installed, it waits for the user to log in to their commercial banking website. The criminals behind Dyre monitor well-known commercial banking websites across the globe and are alerted when an infected user navigates to one of those websites. Once the user is at the banking website login page, Dyre has been known to do one of two things. If the customer account is not protected by two-factor authentication, where the user generates a one-time password from a soft or hard token, the attacker may simply capture the username and password of the user and leverage it to log into the victim's account. The second involves a pop-up message indicating to the user that the website is down. In the latest malware advance, there is an instruction to the victim to call a customer support number. That number connects dialers directly to the cybercriminals who pose as the commercial customer support staff of the bank the victim is trying to access. At this point, the fraudster on the other end of the line will leverage a tactic known as social engineering to coax the user into supplying their username, password and one-time password or token.

Once the attackers have the victim's information, they will leverage the malware installed on the user's computer to connect to the bank website through their network connection. This tactic prevents the bank from identifying that someone is authenticating from a different geographic location and makes it seem that the same, authorized user is authenticating into the bank website. This process is all transparent to the victim, as the fraudsters may still be talking with them on the phone while they work in the background to initiate a wire transaction without the user's knowledge. In the other Dyre attack scenario without the fake customer support call, the victim may also be presented a false "loading" page while the fraudsters initiate the transaction. If the fraudsters identify controls such as dual authorization for wires, the fraudster may then also ask for another secondary authorized user's ID and password to login as that user and approve that same wire.

As you might imagine, the fraudsters on the other end of this conversation are very good at this. It's their job. They spend each day trying to hone their methods to outsmart businesses and their staff. They speak with U.S. English accents and know banking terminology that helps them seem that much more legitimate.

The fallout

The probability of recalling funds from a fraudulent transaction decreases as time goes on. Additionally, no recall attempt is certain to work and businesses are liable for losses due to this kind of account takeover.

Once the attack has been completed, the criminals may also perform what is known as a distributed denial of service attack (DDoS) that will consume network bandwidth; not allowing the victim to authenticate to the banking website or visit any other website for a period of time. The DDoS may cause additional confusion and allow the attackers more time to move the money from their initial account to subsequent offshore accounts to obfuscate the trail of money movement.

The defense

Banks are working to create mechanisms to detect when criminals are fraudulently moving funds; however, you also must be vigilant about your defenses to deter these types of attacks and others.

usbpayment.com