Issued 11/15/17

New IcedID Trojan Targets US Banks

The IcedID Trojan was spotted in September 2017. They said the Trojan has several standout techniques and procedures, such as the ability to spread over a network and the ability to monitor a browser's activity by setting up a local proxy for traffic tunneling. "At this time, the malware targets banks, payment card providers, mobile services providers, payroll, webmail and e-commerce sites in the U.S."

Similar to the TrickBot and Dridex Trojans, IcedID uses both webinjection and redirection attack techniques, researchers said. They said IcedID is being distributed by the Emotet Trojan, which is used as a dropper to put IcedID on targeted systems. Emotet is known for its spam campaigns, designed to look like messages from banks, which contain malicious [.]zip archives. "IcedID possesses the ability to move to other endpoints, and researchers also observed it infecting terminal servers." "Terminal servers typically provide terminals, such as endpoints, printers and shared network devices, with a common connection point to a local area network or a wide area network, which suggests that IcedID has already been targeting employee email to land on organizational endpoints."

To maintain persistence on hosts, IcedID creates a RunKey in the registry of the host's Windows system that allows it to survive reboots. IcedID requires a reboot to complete its full deployment. The reboot also serves as way to attempt to evade analysis via sandboxes that do not emulate rebooting, researchers said.

Once the malware components are in place the victim has their internet traffic redirected through a local proxy that the adversary controls. “The malware listens for the target URL from the list (of financial institutions) and, once it encounters a trigger, executes a designated webinjection. The webinjection sends the victim to a fake bank site set up in advance to match the one originally requested,” researchers wrote. To thwart detection by the end user, the malware redirects traffic at the same time keeping the bank’s correct URL in the address bar. That live connection also means the bank’s correct SSL certificate always shows.