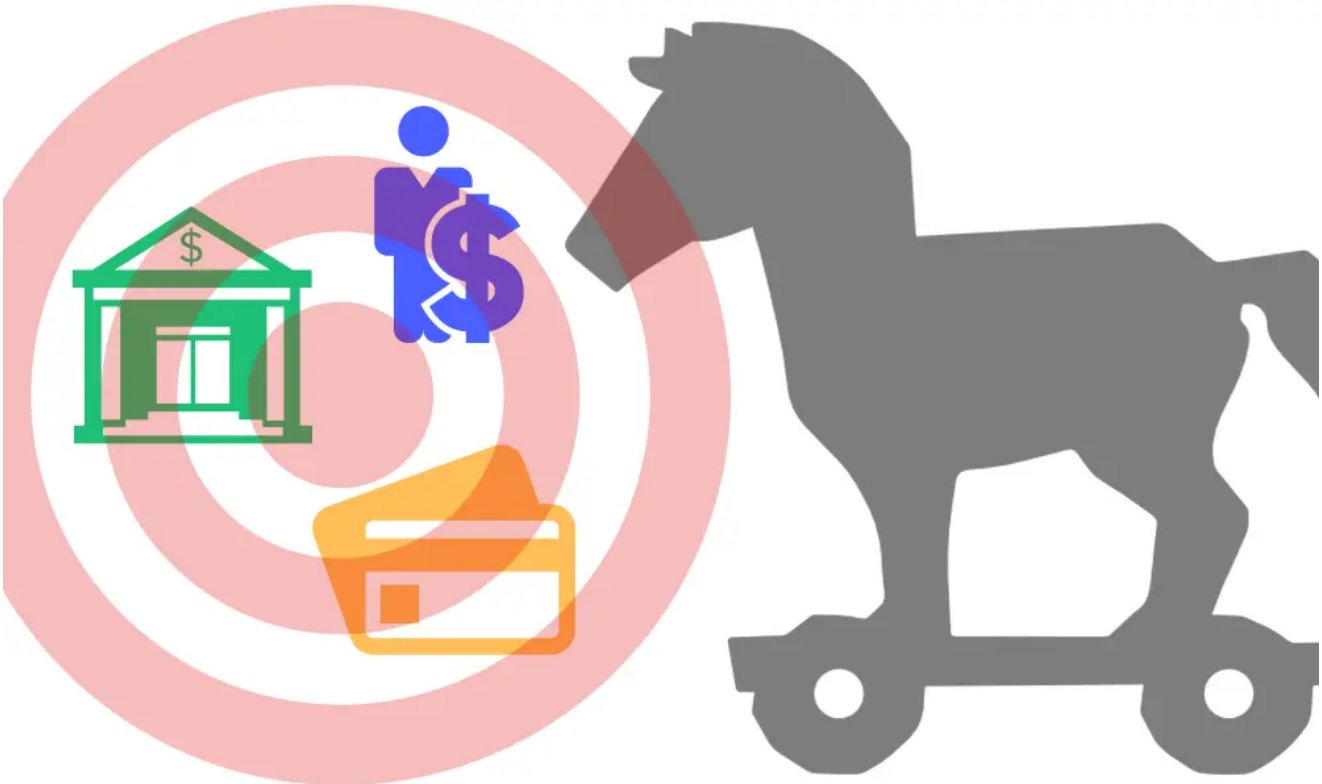
IceID Banking Trojan Targeting Banks, Payment Card Providers, E-Commerce Sites

digitalguardian.com/blog/iceid-banking-trojan-targeting-banks-payment-card-providers-e-commerce-sites

November 14, 2017

Chris Brook Tuesday November 14, 2017



A new banking Trojan, first spotted by researchers in September, has been targeting banks, payment card providers, and mobile services providers, to name a few industries.

Researchers said Monday that a new banking Trojan, IcedID, is still in its infancy but has the potential to rival other big name Trojans, like Zeus, Gozi, and Dridex, in due time.

According to researchers with IBM's X-Force, a division of the company that investigates threats and vulnerabilities, IcedID has been targeting banks, payment card providers, mobile services providers, payroll, and e-commerce websites in the U.S. since September, when it first began making the rounds.

Cybercriminals behind IcedID are using the Emotet loader, spread via malicious spam, to distribute payloads. Emotet isn't new; researchers with Microsoft's Malware Protection Center first spotted it back in 2014. At that time the malware was involved in a spam campaign, mostly against German language speakers and banks, that was stealing account usernames and passwords from email and messaging software.

Developers behind Emotet added new capabilities this past summer to help it propagate and maintain persistence. While the malware still excels at stealing account credentials – from Google accounts, webmail services, even FTP accounts saved in Internet Explorer – it can also take that information to send out phishing emails from compromised accounts.

Like Emotet, IcedID is adept at proliferating; the Trojan keeps tabs on users' online activity via a local proxy for traffic tunneling. It can also jump from endpoint to endpoint, and infect terminal servers like printers and shared network devices via Lightweight Directory Access Protocol, or LDAP, Limor Kessem, an executive security advisor with IBM, wrote Monday.

Like most banking Trojans, GozNym and TrickBot in particular, IcedID uses both webinjection and redirection attacks to perpetrate financial fraud.

The malware downloads a file from its command and control server to help it determine which webinjection attack it will use. Once determined and triggered, the malware executes the webinjection and sends the victim to a phony bank site that mimics the one initially requested. After being tricked into entering their credentials, the attacker controls the session.

The redirection attacks are designed to look "seamless," according to IBM. Instead of shuttling a user off to a new, fake site that has a different URL, the attack displays the legitimate bank's URL in the address bar and the bank's actual SSL certificate.

Researchers suggest that given the similarities of the Trojan, the authors of IcedID may be behind other similar banking Trojans.

"While it is still early to tell how it will fare, its current capabilities, distribution choices and targets point to a group that is no stranger to this domain," Kessem, along with Maor Wiesen, Tal Darsan, Tomer Agayev, co-authors on the report, wrote Monday.

While IcedID certainly seems like it could be poised to take the throne from those other banking Trojans, it’s clear that some, like Dridex, just won't go away.

Earlier this year Dridex adopted a new bypass technique that lets it execute without triggering a Windows UAC alert, it also co-opted a new injection method, known as AtomBombing, to help it evade detection. In April the malware was found being spread in a massive spam campaign that exploited a Microsoft Word zero day. The attacks, which bypassed most mitigaiton efforts, took advantage of the way Microsoft handled OLE2Link objects.

A variant of Dridex just two months ago targeted users of the cloud-based accounting firm Xero. Attackers spooked messages that came from the service, then tricked users into downloading .zip archives containing a JavaScript file that in turn, steals private and personal information.

Chris Brook