Executive Summary

# Inside the World of the Citadel Trojan

By Ryan Sherstobitoff
McAfee Labs

Zeus “banking” malware and its variants have been making headlines in recent months. One variant, the Citadel Trojan, has now taken the spotlight with the news of its withdrawal from the open crimeware market. However, this withdrawal does not necessarily mean that Citadel will cease to be a significant global threat. McAfee Labs research has determined that Citadel’s original developers and perhaps others are developing new variants that significantly extend Citadel’s functionality and threat profile.

The primary trends observed in the second half of 2012 and early 2013 include:

- Targeted attacks on public and private enterprises primarily in Europe
- Functional enhancements used to steal information as well as currency
- Narrowing of targets to a few hundred as compared with tens of thousands of targets observed in previous uses of the Zeus malware family
- Harvesting credentials from internal applications, banking system applications, manufacturing systems, etc. that could be used in a later attack against those applications
- Emergence of the “Poetry Group” as the primary perpetrator of Citadel-based attacks

## Geographic Focus

Unlike most malware attacks, recent Citadel variants have attacked a surprisingly small geographic target with more than 90 percent of known targets based in Europe. But, even within the European theater, the targets have been focused on northern Europe and Spain, as shown in Figure 1.

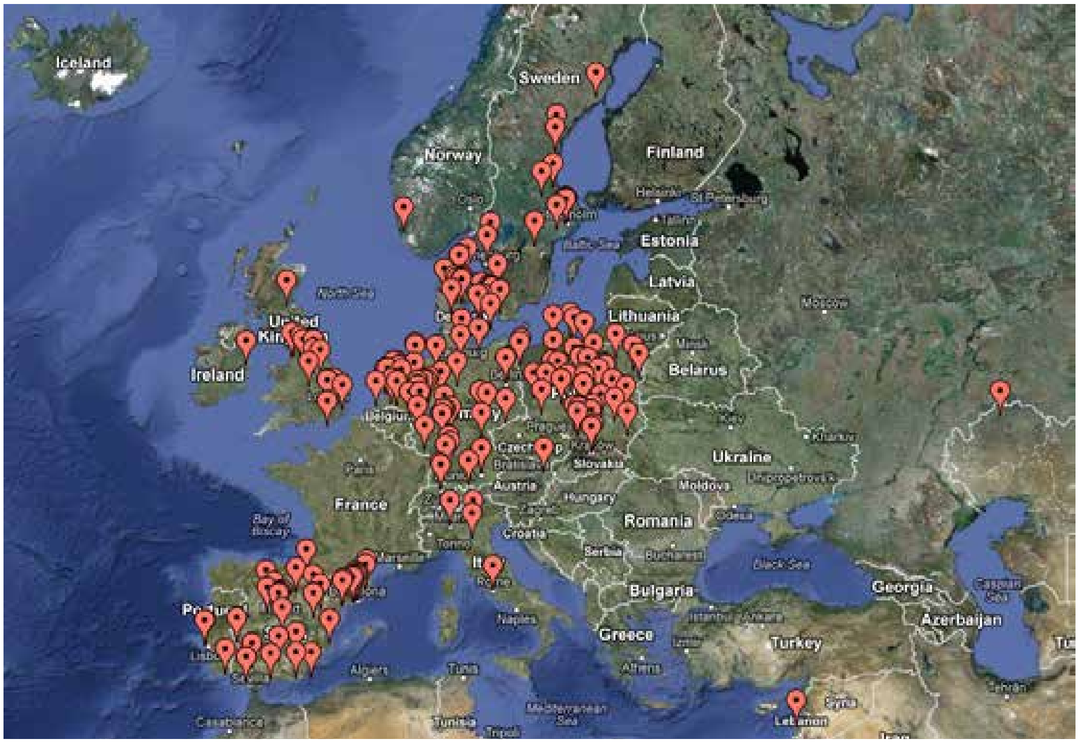

Figure 1. Proliferation of Citadel in Europe.

Additionally it’s clear based on our telemetry data that the gangs using Citadel are not targeting consumers in general; rather, the targets are businesses and government entities.

## Functional Extensions

The Zeus malware platform was originally designed to steal currency, frequently in small amounts from thousands of victims. Citadel's developers, however, have clearly recognized that sometimes data, particularly authentication credential data, can be more valuable than currency. Consequently, in the second half of 2012 we began to see Citadel variants designed to penetrate local government and large private enterprise IT infrastructure.

The Poetry Group, which distinguishes itself by embedding snippets of old English–style poetry in their Citadel variants, has been particularly active in attacking large private enterprises, as shown in Figure 2. Attacks against public sector targets have been particularly pronounced in Poland, where Citadel has been used to penetrate local/city government data repositories. McAfee Labs researchers have also uncovered new financial fraud functionality built into Citadel written entire in JavaScript that appears to target employees of the public sector agencies under attack.

Recently deployed Citadel variants now have features that extend beyond simple bank fraud. The malware can collect anything from a victim's PC. Citadel Version 1.3.45, the "Extreme Edition," contains functionality allowing a simplified remote control connection to the victim. In other words the Trojan will establish (automatically if need be) from the control panel a hidden channel of communication with the victim's PC. Version 1.3.45 also has a feature that will automatically establish a remote connection with botnets that are online, making it possible to script attacks against different targets. The most recently discovered Citadel variants also have built-in DNS redirect functionality that prevents infected systems from contacting the websites of major IT security vendors and global law enforcement agencies.

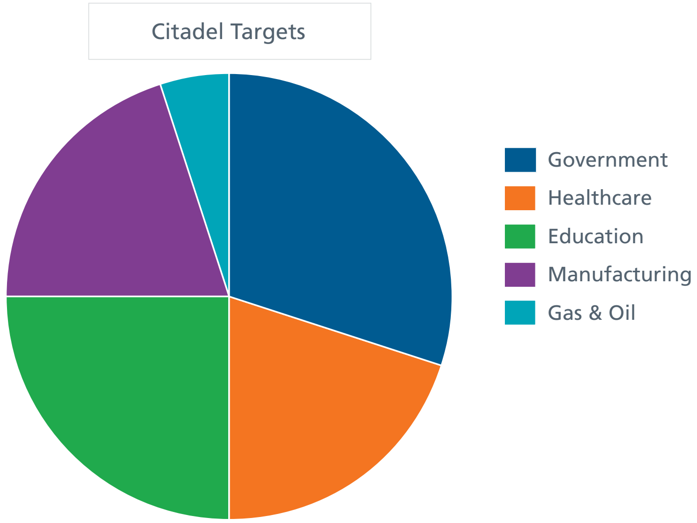

Figure 2: Poetry Group targets by industry sector.

## Reduced Target Volume

The vast majority of global malware attacks rely on the "Law of Large Numbers" for their success. The basic theory is that if you attack enough targets you'll eventually find enough that are vulnerable to extract the currency or information of interest. Recent Citadel attacks have taken the opposite approach.

In a Citadel attack observed between December 22, 2012, and January 6, 2013, McAfee Labs telemetry identified a total of 156 victims in only four countries, as shown in Figure 3.

| Country | Number of Infected Victims |
|---|---|
| Poland | 71 |
| Denmark | 44 |
| Sweden | 29 |
| Spain | 12 |

Figure 3. Citadel Campaign #1 targets by country.

## Poetry Group

The most active group perpetrating Citadel-based attacks is known as the Poetry Group. This group embeds somewhat poetic strings of text written in old English in the Citadel binaries used in the attacks. This characteristic has been found consistently among the binaries and contains certain paragraphs of text that appear in memory associated with the malicious process running. These strings do not appear in other campaigns that have been observed in Europe; thus we can determine a specific group is behind these campaigns. When one of the variants used in an active campaign makes mention of Denmark specifically, Denmark is one of the countries targeted in this attack.

## Conclusion

Citadel is considered an emerging threat to not only the financial services industry, but to other industries as well. Citadel gives cybercriminals advanced remote connectivity, and it also gives them the ability to dynamically decide which target to engage.

While Citadel is being withdrawn from the open market, McAfee Labs believes that we will continue to see successor variants deployed throughout 2013. We also expect that its targets will expand as more cybercriminals realize the potential capabilities of Citadel go well beyond financial fraud. There is a significant amount of recent activity to suggest that perpetrators will continue to use Citadel to attack businesses and government organizations globally.

A copy of the full report can be found here: http://www.mcafee.com/us/resources/white-papers/wp-citadel-trojan.pdf.

McAfee
An Intel Company

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com