



Posts Tagged 'russia'

Tornado Malware Kit

Thursday, March 5th, 2009

In this post, we will be taking a look at the Tornado Malware kit. Tornado is a Russian web-attack kit used by hackers to compromise as many machines as possible. "Out of the box," it comes with 14 exploits, although users have space to add more, thanks to a modular design (handy!). Visitors are greeted with the following login prompt:



The spelling throughout the application is generally poor. After login, users are taken to the stats page (a dashboard of sorts) which shows information about the traffic the kit has seen so far, broken down by OS and web browser. The Tornado kit has a target URL which attackers direct as much traffic to as possible. Once an attacker is able to lure a visitor to the malicious URL, Tornado chooses an exploit most likely to succeed and serves it up. It does this by analyzing the visiting browser's User-Agent header. Here we can

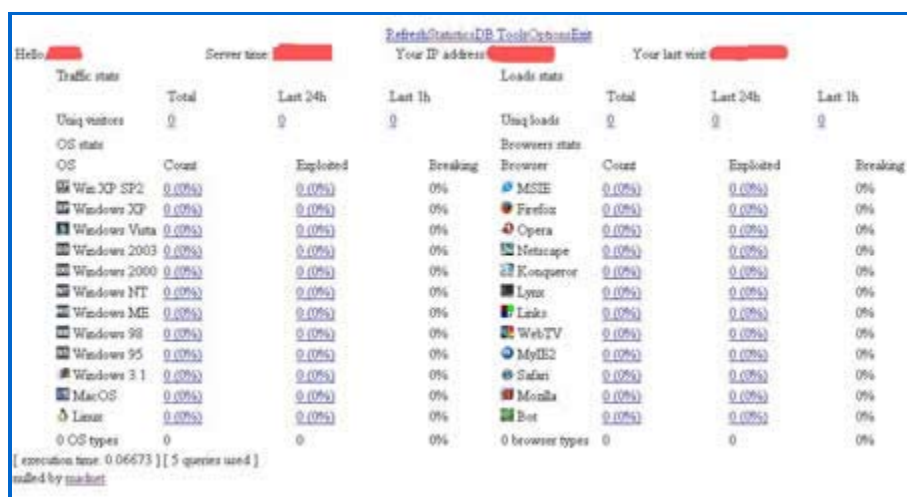
```

74 setcookie( "it", $owner, $time, $time + $lifetime );
75 $uagent = $_SERVER['HTTP_USER_AGENT'];
76 $version = "";
77 if ( strpos( $uagent, "Opera" ) )
78 {
79     $browser = 1;
80     $step = explode( " ", substr( $uagent, strpos( $uagent, "Opera" ) + 6 ) );
81     $version = $step[0];
82 }
83 else if ( strpos( $uagent, "MSIE" ) )
84 {
85     $browser = 1;
86     $step = explode( ":", substr( $uagent, strpos( $uagent, "MSIE" ) + 5 ) );
87     $version = $step[0];
88 }
89 else if ( strpos( $uagent, "Firefox" ) )
90 {
91     $browser = 2;
92     $step = explode( " ", substr( $uagent, strpos( $uagent, "Firefox" ) + 6 ) );
93     $version = $step[0];
94 }
95 else if ( strpos( $uagent, "Ie" ) || strpos( $uagent, "Internet Explorer" ) )
96 {
97     $browser = 4;
98 }
99 else if ( strpos( $uagent, "Konqueror" ) )
100 {
101     $browser = 5;

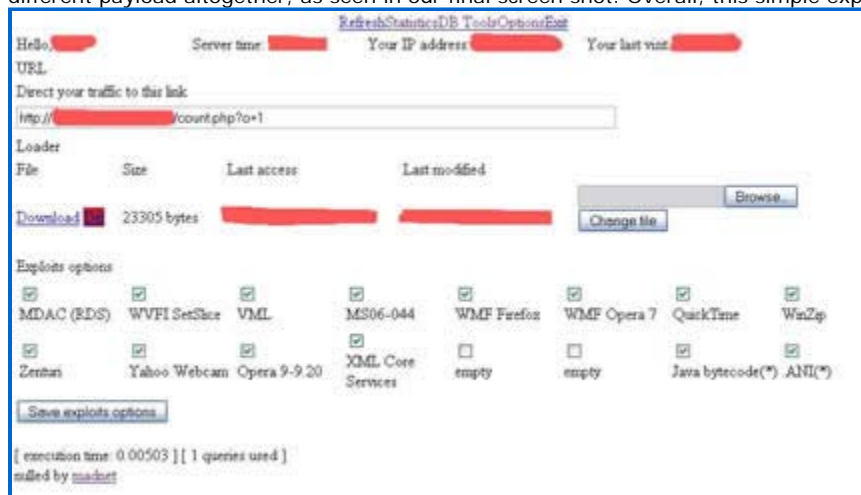
```

see part of that process:

In some cases, attackers place the link into other compromised sites, so that visitors may have no idea they are browsing a malicious site. Buried in the obfuscated code, several requests are made to Russian web sites. This allows the author of the kit to monitor where the kit is used, and make sure that it is being used, you know, "legally".



If the browser exploit attempt is successful, the victim's machine will make a request to download an EXE from the attacker's site. At this point, it is game over. The loader that Tornado uses is configurable, so it's easy to add additional payloads, or change to a different payload altogether, as seen in our final screen shot. Overall, this simple exploit kit has some worrisome capabilities.



Share This Blog | [SlashDot](#) | [del.icio.us](#) | [Technorati](#) | [Reddit](#) | [Digg it](#)

Kyrgyzstan Under DDoS Attack From Russia

Wednesday, January 28th, 2009

"The Cyber Attack No One Is Talking About"

Since JANUARY 18, 2009, the two primary Kyrgyzstan ISPs (www.domain.kg, www.ns.kg) have been under a massive, sustained DDoS attack almost identical in some respects to those that targeted Georgia in August 2008. Few alternatives for Internet access exist in Kyrgyzstan. With just two smaller ISPs left to handle the load, these attacks from Russian IP address space^{1,2} have essentially knocked most of the small, Central Asian republic offline.

Some believe that this is a way to silence rhetoric from a new and relative powerful opposition coalition whose primary aim is the removal of current government officials, especially Kyrgyz President Kurmanbek Bakiyev³, and a break from the administrations policies.

On the other hand, others think these attacks are part of a Russian campaign to pressure Kyrgyz President Kurmanbek Bakiyev to close US access to a key airbase, which intensified on the same day as the DDoS attacks. That airbase is a key resource in the war against Islamist militants in Afghanistan.

In remarks after meeting then Secretary of State Condoleezza Rice in 2005, Bakiyev seemed willing to allow US and UN forces to

continue to use the base⁴:

"... that the coalition air base in international Manas airport will be [available] until the situation in Afghanistan is completely stabilized..."

- Kyrgyz President Kurmanbek Bakiyev

(via Russian translator)

In December 2008, however, Kyrgyz officials announced that they would begin plans to phase out the use of the airbase. The US has denied that any such plans were being made.

Now, under renewed pressure from Russia, sources from inside Bakiyev's administration indicate that the decision to close the base to US and UN forces has already been made, and a public announcement is forthcoming⁵.

Russia is prepared to offer Kyrgyzstan a \$300 million USD loan and provide \$1.7 billion USD of investment in the energy sector of the former Soviet republic. Kyrgyz President Bakiyev is scheduled to meet with Russian officials in charge of the deal in Moscow on February 3, 2009. The Russians have indicated that the deal is dependent on the ousting of foreign forces from the Central Asian country's airbase.

Suppression of the opposition movement's views, especially the ability to make their point internationally via the Internet, certainly makes sense for Russia. Russia operates the only other airbase in Kyrgyzstan and wants a monopoly on air power in what they term their own back yard. However, US use of the Manas airbase is a source for a steady inflow of cash to the ailing Kyrgyz economy. The opposition's position is that the Russian deal is risky and that it would be better for Kyrgyzstan's economy overall to stay the course, to continue to allow the US and Russia to operate from their own separate airbases. The DDoS attack would be one way to keep the opposition from publicizing their alternative and gaining support for it. That could result in opposing diplomatic pressure from the US and its allies.

"Cyber-attacks are part of the information war, making your enemy shut up is a potent weapon of modern warfare."

- Alexander Denezhkin, editor at Cybersecurity.ru

August 2008

DDoS attacks by Russia's cyber militia seem to be a standard part of campaigns against other nations that are friendly to Russia's Western rivals on a variety of issues, including energy, economic investment, politics, and the military.

In the past, Russian officials have stated that they rely on the recruitment of technically capable Russian citizens to assist them in these types of operations. Many believe that the catalyst for this mobilization is, at least in part, unofficial requests from Russian authorities passed down their contacts in Russia's cyber underground. The use of cyber militias puts distance between the Russian government and shelters the it from culpability for the peacetime use of information warfare tactics. There is often a combination of motives. Couple the lack of culpability with the "bang for the buck" in using DDoS as a means to an end in policy and military matters, it's a win-win proposition for the Russians. As long as that remains true, we expect to see this pattern repeat. With each new exercise, the cyber militia matures and their capabilities grow. Since 2005, cyber attacks attributed to Russia's cyber militia have increased in frequency. This is a pattern of escalation.

These attacks are powerful tools wielded by Russia's cyber militia against the friends and allies of the United States. Is this action so expected, the pattern so established — Israel, Ukraine, Estonia, Lithuania, and Georgia — that it fails to garner due attention? With modern worms capable of quickly building 1+ million strong botnet armies, will we have countermeasures and contingency plans in place when the cross hairs lock-on to our own infrastructure?

-
1. <http://www.palantirtech.com/greygoose/>
 2. <http://intelfusion.net/wordpress/?p=509>
 3. <http://www.eurasianet.org/departments/insightb/articles/eav012109a.shtml>
 4. <http://www.state.gov/secretary/rm/2005/54678.htm>
 5. <http://www.smh.com.au/news/world/russia-presses-kyrgyzstan-to-close-us-base/2009/01/18/1232213448844.html>

Note: The US State Department has removed the remarks between Sec. Rice and Kyrgyz President Bakiyev from their web site. A copy was located in Google's cache [here](#)

Share This Blog |  [SlashDot](#) |  [del.icio.us](#) |  [Technorati](#) |  [Reddit](#) |  [Digg it](#)

Beginning of the end for EstDomains

Monday, November 3rd, 2008

If you're a hacker wanting to register a domain for nefarious purposes, EstDomains is your go-to guy. They registered tens of thousands of malicious domains during their existence, providing an integral piece of the malware lifecycle. The **Russian Business Network (RBN)** used them extensively for their "bullet proof" hosting (web hosting designed to make takedowns extremely difficult if not impossible). Back in February of this year Vladimir Tsastsin, EstDomains founder, was sentenced to three years in prison for forgery, money laundering and credit card fraud. This conviction caused EstDomains to break section 5.3 of ICANN's Registrar Accreditation Agreement. This section states:

Any officer or director of [a] Registrar is convicted of a felony or of a misdemeanor related to financial activities, or is adjudged by a court to have committed fraud or breach of fiduciary duty, or is the subject of judicial determination that ICANN deems as the substantive equivalent of any of these; provided such officer or director is not removed in such circumstances.

On October 28th, ICANN notified EstDomains that on November 12th, 2008, it would no longer be an accredited registrar. ICANN has posted this notice here: <http://www.icann.org/correspondence/burnette-to-tsastsin-28oct08-en.pdf>

EstDomains is currently attempting to distance themselves from Tsastsin in an attempt to stay in business. They responded to ICANN claiming Tsastsin was removed from his position in January one month before his conviction on the 29th: <http://www.icann.org/correspondence/poltev-to-burnette-29oct08-en.pdf>

Due to this response October 29th ICANN stayed the termination process: <http://www.icann.org/en/announcements/announcement-2-29oct08-en.htm>

Hopefully ICANN will make the right decision and shutdown these criminals for good.

Share This Blog |  [SlashDot](#) |  [del.ico.us](#) |  [Technorati](#) |  [Reddit](#) |  [Digg it](#)

SecureWorks Blogs

Other SecureWorks Blog Categories:

- [General](#) (25)
- [Links](#) (7)
- [Phishing](#) (3)
- [Research](#) (68)
- [Spam](#) (1)
- [Trojans](#) (4)

Blogs by Month:

- [March 2009](#)
- [February 2009](#)
- [January 2009](#)
- [December 2008](#)
- [November 2008](#)
- [October 2008](#)
- [September 2008](#)
- [August 2008](#)
- [July 2008](#)
- [June 2008](#)
- [May 2008](#)
- [April 2008](#)
- [March 2008](#)
- [February 2008](#)
- [January 2008](#)
- [December 2007](#)
- [November 2007](#)
- [October 2007](#)
- [September 2007](#)
- [August 2007](#)
- [July 2007](#)
- [June 2007](#)
- [May 2007](#)
- [March 2007](#)
- [January 2007](#)
- [December 2006](#)
- [November 2006](#)
- [October 2006](#)
- [September 2006](#)
- [August 2006](#)
- [June 2006](#)
- [May 2006](#)

Printed from <http://www.secureworks.com>

For more information, please call (877) 905-6661 or email info@secureworks.com.
