Anti-Abuse Policy

Domain Name Anti-Abuse Policy

The following policy is announced pursuant to Public Interest Registry Registry-Registrar Agreement ("RRA") in effect between Public Interest Registry and each of its Registrars, and is effective February 5, 2009, August 22, 2013 or February 28, 2014 as applicable.

Abusive use(s) of .org, .co, and .亚洲 domain names should not be tolerated. The nature of such abuses creates security and stability issues for the registry, registrars and registrants, as well as for users of the Internet. In general, Public Interest Registry defines abusive use of a domain as the wrong or excessive use of power, position or ability, and includes, without limitation, the following:

- **Illegal or fraudulent actions**
- **Spam**: The use of electronic messaging systems to send unsolicited bulk messages. The term applies to e-mail spam and similar abuses such as instant messaging spam, mobile messaging spam, and the spamming of Web sites and Internet forums. An example, for purposes of illustration, would be the use of email in denial-of-service attacks
- **Phishing**: The use of counterfeit Web pages that are designed to trick recipients into divulging sensitive data such as usernames, passwords, or financial data
- **Pharming**: The redirecting of unknowing users to fraudulent sites or services, typically through DNS hijacking or poisoning
- **Willful distribution of malware**: The dissemination of software designed to infiltrate or damage a computer system without the owner's informed consent. Examples include, without limitation, computer viruses, worms, key loggers, and Trojan horses
- **Fast flux hosting**: Use of fast-flux techniques to disguise the location of Web sites or other Internet services, or to avoid detection and mitigation efforts, or to host illegal activities. Fast-flux techniques use DNS to frequently change the location on the Internet to which the domain name of an Internet host or name server resolves. Fast flux hosting may be used only with prior permission of Public Interest Registry
- **Botnet command and control**: Services run on a domain name that are used to control a collection of compromised computers or “zombies,” or to direct denial-of-service attacks (DDoS attacks)
- **Distribution of child pornography**
- **Illegal Access to Other Computers or Networks**: Illegally accessing computers, accounts, or networks belonging to another party, or attempting to penetrate security measures of another individual's system (often known as “hacking”). Also, any activity that might be used as a precursor to an attempted system penetration (e.g., port scan, stealth scan, or other information gathering activity)

Pursuant to Public Interest Registry's Registry-Registrar Agreement(s), Public Interest Registry reserves the right to deny, cancel or transfer any registration or transaction, or place any domain name(s) on registry lock, hold or similar status, that it deems necessary, in its discretion; (1) to protect the integrity and stability of the registry; (2) to comply with any applicable laws,
government rules or requirements, requests of law enforcement, or any dispute resolution
process; (3) to avoid any liability, civil or criminal, on the part of Public Interest Registry, as well as
its affiliates, subsidiaries, officers, directors, and employees; (4) per the terms of the registration
agreement or (5) to correct mistakes made by Public Interest Registry or any Registrar in
connection with a domain name registration. Public Interest Registry also reserves the right to
place upon registry lock, hold or similar status a domain name during resolution of a dispute.

Abusive uses, as defined above, undertaken with respect to .org, .opr, .⌘⌘, and . порядке domain
names, shall give rise to the right of Public Interest Registry to take such actions under Public
Interest Registry's Registry-Registrar Agreement(s) in its sole discretion.
Frequently Asked Questions
Quickly find answers to the most commonly asked questions

- What is Dynamic DNS?
- What is a Hostname?
- What is an IP address?
- Can I make my own update client?
- What is DNS?
What is a Dynamic IP Address?

What is a Static IP Address?

Why did my free hostname expire or get deleted?

What is Port Forwarding?

What DNS Servers do I use with Plus Managed DNS?

What are the benefits of upgrading to Enhanced Dynamic DNS?

What does No-IP do?

What if No-IP isn't an integrated solution in my router or device?

What forms of payment do you accept?
Report Abuse
If you believe the actions of one of our users violates our Terms of Service, please inform us immediately at:

[abuse@no-ip.com](mailto:abuse@no-ip.com)

Contact Support
+1 775.853.1883
+1 877.367.6647 (inside the US)
+1 775.853.1886 (fax)

Monday-Friday
6:30am - 5:30pm PT

Helpful Links
› Getting Started
› Tools
› Open a Ticket
› Contact

Get Connected

Translate

Copyright © 2013 • No-IP.com • All Rights Reserved
Support Home / FAQs / Knowledge Base / Tips & Announcements / Download
On the trail of malicious dynamic DNS domains

OpenDNS Security Labs

- opendns.com
- Search

- Big Data
- Blog
- About Us

OpenDNS Security Labs » OpenDNS Security Labs Blog » April 2013 » On the trail of malicious dynamic DNS domains

April 15, 2013

By Dhia Mahjoub

Dynamic DNS is a useful technology that allows a domain name to point to Internet resources hosted on changing public IP addresses. Consider an individual or small business with a dynamic IP who needs to provide consistent content or services publicly advertised to the outside world via a domain name (e.g. website, FTP server, mail server, game room, webcam monitoring, etc). That’s where dynamic DNS helps out. Typically, these customers use the IP assigned to them by their ISP, and every time their IP changes, they notify their dynamic DNS provider to update its name servers so that the customer’s domain points now to the new IP. The notification happens through a client software installed on the customer’s router/computer or via an HTTP restful API. One such client software is DNSOMATIC by OpenDNS.

Unfortunately, the convenience of dynamic DNS did not go unnoticed by miscreants, who have been abusing free, dynamic DNS to perform various attacks such as large-scale malvertising, and targeted

http://labs.opendns.com/2013/04/15/on-the-trail-of-malicious-dynamic-dns-domains/
spear-phishing, which both resulted in drive-by downloads, and use it for botnet C&C. For attackers, using dynamic DNS constitutes another agile evasion technique against IP blacklisting. It also allows them to deliver malicious payloads from constantly-changing hosting IPs, be it infected individuals’ computers or compromised public websites. To circumvent domain blacklisting, attackers can also use randomly-generated disposable subdomains under the dynamic DNS domain to point to the next hop in a redirection chain or to the final malware hosting IP. This seems similar to fast flux, although from a definition standpoint they are different. For dynamic DNS, the dynamic IP is supposed to fall in the IP range of the ISP (1 or a few ASNs), whereas, with fast flux, a domain will be pointing to an increasing number of different IPs scattered across numerous ASNs and multiple geographical locations. Additionally, for dynamic DNS, the authoritative name servers for a dynamic DNS domain physically belong to the dynamic DNS provider, whereas with fast flux, double fluxing is possible where the name servers can be made point to constantly changing IPs of physical hosts located in disparate ASNs and countries. In practice, dynamic DNS domains map to a much smaller set of IPs than fast flux.

In this blog, we discuss the relationship between dynamic DNS domains and malware as we see it through mining our large DNS data sets. This can also give some perspective on how to address the problem of rogue dynamic DNS domains.

**Dynamic DNS analysis**

There are plenty of dynamic DNS providers, both free and for a cost. One good list of them is available [here](http://labs.opendns.com/2013/04/15/on-the-trail-of-malicious-dynamic-dns-domains/). Dynamic DNS providers offer users to either register domains (2LDs), or subdomains (3LDs) under a predefined set of domains (2LDs). For instance, changelP.com has a list of 155 domains, under which a user can freely register any subdomain of his choice (if it is available). For example, they have 1dumb.com and 2waky.com as pre-registered domains, and a user can register the hostnames johndoe.1dumb.com or myhomebusiness.2waky.com. changelP also offers to users to register a domain under the following TLDs .com, .net, .info, .org, .biz, or .us. This latter choice requires an annual registration fee though. Similar offers are available from other providers like no-ip.com, afraid.org, Dyn.com (formerly known as DynDNS), etc. The common practice for attackers is to abuse the free subdomains.

For this study, we are interested in evaluating the amount of dynamic DNS domains we see in our daily authoritative DNS traffic and the percentage of malicious domains within, and also find out which subdomains are the most frequently abused.

First, we collect a sample of known malicious dynamic DNS domains, then, we compile a list of known pre-registered domains offered by a few dynamic DNS providers. For the malicious sample, the dynamic DNS providers that are mostly used are sitelutions.com, noip.com, changelip.com, and dnsdynamic.org. For the general list, we select known dynamic DNS providers such as: changelip.com, dnsdynamic.org, noip.com, freedns.afraid.org, dyndns.com, sitelutions.com, and 3322.org. These samples are not exhaustive as there are a lot more dynamic DNS providers (and more of them are abused). Some dynamic DNS providers are not limited to offering dynamic DNS services and act also as regular domain registrars, so a domain registered with a dynamic DNS provider and using its name servers might not necessarily be using the dynamic DNS service. We think, however, that these samples are representative enough for the sake of the analysis.
Next, we resolve the NS (name servers) of all domains in both samples. This list of name servers will be used to filter out the daily logs to identify domains using dynamic DNS. The logic here is that if we already know about a set of dynamic DNS domains, we can identify their name servers, and any new domain that uses these latter name servers will be assumed to be a dynamic DNS domain. The name servers from the general list give a trend on the percentage of total dynamic DNS domains in daily traffic, whereas, the name servers from the malicious sample provide an idea on the dynamic DNS traffic most likely to be malicious. The name servers associated with the sample of malicious dynamic DNS domains are: ns[1-3].changeip.org, ns[1-5].changeip.com, ns[1,2].dnsdynamic.org, nf[1-5].no-ip.com, and ns[1-5].sitelutions.com.

In the next step, we collect sample authoritative DNS logs from three resolvers in London, Ashburn and Singapore, where we have for every domain, its associated authoritative name server(s). For each day, we collect a sample of 1,518,782 domains on average with their name servers data. We collect logs for a week, then for each day, we identify those domains whose name servers fall within the list of name servers of dynamic DNS providers.

Finally, we compare the identified dynamic DNS domains against our blacklist (which is constantly updated with new data), and we show the results in the figures below. For the sake of this discussion, we call sortecielo.2waky.com a hostname, or subdomain or 3LD and 2waky.com a domain or 2LD. We can see in the figures, that there are 30,000+ dynamic DNS hostnames (3LDs) observed daily in the sample authoritative DNS traffic, and 3000+ corresponding domains (2LDs). For the same period, out of the same daily domain sets, we identify 1400+ malicious hostnames, and 200+ associated domains every day. This gives an idea about the density of the associations between a domain and its “children” subdomains.
Top abused dynamic DNS domains

In the following tables, we show the top 20 domains observed in daily traffic over a week as well as the top 20 domains used for malicious purposes over the same period. The counts next to the domain represent the number of hostnames under that domain. For example, on the first day, disqus had 18,294 hostnames of the form subdomain.disqus.com

In the next table, we show side by side, for a single day the top 20 dynamic DNS domains in general traffic and those that had malicious hostnames. We indicate in red, those domains that are present in

http://labs.opendns.com/2013/04/15/on-the-trail-of-malicious-dynamic-dns-domains/
both top malicious domains and top popular domains in a daily DNS traffic i.e. no-ip.org, no-ip.biz, no-ip.info, hopto.org, dlinkddns.com, myftp.org, myvnc.com, myftp.biz, and us.to. What is noteworthy is that some popular dynamic DNS domains for general legitimate uses are also the top ones abused for malicious purposes. This makes blocking the entire domain a little tricky as that would deny visibility to a lot of legitimate content. Notice that the dynamic DNS provider no-ip.com is the most used one for both legitimate and malicious intent. The domains no-ip.org, no-ip.biz, no-ip.info, hopto.org, myftp.org, myvnc.com, and myftp.biz all use no-ip name servers. The right hand table for top malicious domains is illustrated at the end of this blog as a graph representation.

![Graph representing top malicious domains]

[top 20 domains in general traffic on the left, and top 20 malicious domains on the right]

In the next table, we show the percentage of malicious usage of hostnames under each domain. For example, 56.71% of the 3LDs under hopto.org are malicious. Clearly, some domains are heavily used for malicious purposes.

<table>
<thead>
<tr>
<th>hopto.org</th>
<th>no-ip.org</th>
<th>no-ip.info</th>
<th>no-ip.biz</th>
<th>myftp.org</th>
<th>us.to</th>
<th>myvnc.com</th>
<th>dlinkddns.com</th>
<th>myftp.biz</th>
</tr>
</thead>
<tbody>
<tr>
<td>56.71</td>
<td>4.57</td>
<td>10.70</td>
<td>3.90</td>
<td>37.50</td>
<td>49.45</td>
<td>33.33</td>
<td>12.22</td>
<td>20.20</td>
</tr>
</tbody>
</table>

Below, we show an illustrative graph of the mapping of hostnames to domains taken from the list of detected malicious dynamic DNS domains of one day. The largest connected component on the top left corner is that of the domain hopto.org which has 245 malicious 3LDs associated with it, e.g. spilak.hopto.org, arasispodmoonf.hopto.org, 1n12.hopto.org, etc. On the right of hopto.org is the cluster of no-ip.org with 125 malicious 3LDs, then no-ip.info on the right with 103 hostnames, etc.
We further took a sample of hostnames under hopto.org, and we determined that they were used to serve urls for Fragus Exploit kit, Best Pack Exploit kit, Incognito Exploit kit, Java and PDF exploits, leading to Trojan Fake AVs downloads. They were also used as CnC for W32/Dorkbot-EK, Rogue:Win32/Winwebsec, Trojan-Ransom.Win32.Mbro.ysw, IRC botnets, and also to serve phishing urls. In another sample, we observe that malicious dynamic DNS domains are massively associated with Blackhole exploits kit, Neosploit exploits, PDF exploits, and other exploits leading to the delivery of rogue antivirus, trojans, Backdoor SDBot, etc. It is worth mentioning that it is difficult to trace back the registration information of dynamic DNS domains that are in the form of subdomain. [predefined domain].tld because the whois information only records the registration information of the domain (the 2LD).

Note: The tools and platform I used for this study are our Hadoop dev cluster, Apache Pig, Python, and Unix shell tools (sed, awk, grep, etc).
At No-IP, we have a very strict abuse policy. Our abuse team is constantly working to keep our domains free of spam and malicious activity. We have filters that block certain words and we scan our network daily for signs of malicious activity. Even with such precautions, our services do fall prey to cyberscammers and spammers. We highly encourage our users and others to let us know if they come across a hostname that isn't abiding by our Terms of Service. We dislike spammers and scammers just as much as everyone else. To report a violation of our TOS or any other abuses of our services, please email abuse@no-ip.com.
• RSS

Recent Posts

• SANS Digital Forensics and Incident Response Summit Recap
• Why Using Real World Data Matters for Building Effective Security Models
• CnC? Botnet? Speak English Already!
• Source Boston 2014
• Realistic Network Rendering with PovRay

Archives

• June 2014
• May 2014
• April 2014
• March 2014
• February 2014
• January 2014
• December 2013
• November 2013
• October 2013
• September 2013
• August 2013
• July 2013
• June 2013
• May 2013
• April 2013
• March 2013
• February 2013
• January 2013
• December 2012
• November 2012
• October 2012
• September 2012
• August 2012
• July 2012
• June 2012
• May 2012
• April 2012
• March 2012

• Spiceworks
• Twitter
• Google+
• Facebook
• LinkedIn

• Terms of Service
• Website Terms of Use
• Privacy Policy
Two weeks ago we briefly discussed the role of dynamic DNS (DDNS) in a Fiesta exploit pack campaign. Today we further analyze and explore the role of DDNS in the context of cyber attack proliferation and present the case for adding an operational play to the incident response and/or threat intelligence playbook to detect attack pre-cursors and attacks in progress.
Managements’ Bottom Line

There are over fifty DDNS providers that leverage over one thousand combined domains to offer free and fee-based accounts. DDNS is a useful service with numerous legitimate applications. One of the primary DDNS use cases involves enabling connections to networks that rely on dynamic IP address ranges. Dynamic IP addressing tends to be more ubiquitous on residential networks, thus when home Internet users wish to host a website or connect to their home Virtual Private Network (VPN), they often rely on a DDNS service. The service itself maps a new sub-domain (based on a list of existing domains owned by the DDNS provider) to the IP address currently provisioned by the Internet Service Provider (ISP) and automatically changes the IP address as lease times expire and the ISP assigns a new IP address to the residential customer.

The 2014 Cisco Annual Security Report addresses the need for a threat-centric detection model and we believe DDNS is a perfect example of benefiting from attacker methodology analysis. Like all good and useful Internet services, threat actors (across the motivation spectrum) have co-opted DDNS for nefarious purposes. In order to launch an attack that involves malicious code (malware) that maintains a persistent connection to a command and control (C2) server, or for data exfiltration from a victim network, an attacker must first configure basic Internet infrastructure and DNS is a primary consideration in the larger decision process.

Choices include: domain or IP address, register domains with a stolen credit card or compromise a legitimate registrar account and create new DNS records, or finally use a free DDNS service. Obviously forgoing a domain and hard coding traffic to an IP address reduces attack flexibility since the server may be quickly identified and disabled. Registering a domain with a stolen credit card is sub-optimal for longer duration attacks since the registrar will disable the domain and account once the card fraud is discovered. Compromising an existing registrar customer account is resource intensive and does not scale well for attacks requiring multiple domains.

Free DDNS services, by comparison, check all of the necessary attack boxes. Sub-domains can be quickly and easily
generated and DNS records are trivially changed. For the remote access Trojan (RAT) crowd that are typically attempting to spy on female victims and running servers from home, DDNS is a natural fit. In fact, searching the web for tutorials on using freely available RATs like Black Shades, Dark Comet, or Poison Ivy returns results that all instruct RAT attackers to first create DDNS sub-domains in order to properly configure the RAT, specifically enabling a “back connect” to the attacker. Naturally, one segment of RAT users tend to be less technical, relying on tutorials and point and click interfaces to actually launch the RAT, which likely contributes significantly to the overall metrics of malicious DDNS use.

Speaking of metrics, let’s dig into the malicious DDNS numbers from our Internet vantage point. The following graph illustrates the Cloud Web Security (CWS) percentages of specific DDNS base domains that are blocked based on web reputation scores. As you can see the DDNS block rate average is nearly 20% while the average block rate for all other web traffic is less than 1%. There are also quite a few DDNS base domains that are blocked with almost 100% frequency (the reputation charts below exclude DDNS domains that are blocked 100% of the time).
Next up are the block statistics from anti-virus detection. Unfortunately there are fewer blocks overall, and the DDNS block rate average is greater than 0.2% as compared with the much lower 0.001% average block rate for all web traffic.

The top ten Kaspersky verdicts for DDNS domain blocks appear below and contain heavy emphasis around Java exploits and JavaScript redirection.
Last, the word cloud below depicts the top DDNS base domain offenders. The size of the word indicates total CWS traffic observed and the darker color indicates a higher percentage of web reputation blocks.
We have established that the CWS block rate for DDNS domains is on average substantially higher than for all other web traffic, but what do the corresponding malware numbers look like for the DDNS domains most abused by threat actors?
The prolific use of DDNS specifically for malware campaigns represents a significant indicator of compromise (IoC) category. While legitimate DDNS use cases exist, implementing detection around DDNS traffic in the enterprise is crucial because it is a preferred threat actor tool. This operational alert is bound to generate noise in the form of false positives, but given the above metrics, this category is too important to ignore.

**The Network Security Monitors’ Operational Insight**

The malware counts per DDNS domain are informative, but obviously the hashes themselves are much more instructive so we include the specific SHA1 hashes corresponding to the malware (observed since 2009) for the top DDNS base domain counts above. VRT incorporated the following hashes into their detection cloud to provide coverage across multiple tools including ClamAV and FireAMP:

- adultdns.net
- servehttp.com
- myvnc.com
- redirectme.net
- hopto.org
- zapto.org
- no-ip.info
- no-ip.biz (zip file due to file size)
- no-ip.org
- sytes.net
- adultdns.net-samples
Deeper inspection of a randomly selected sample from the DDNS malware set reveals TCP traffic from victim hosts back to fuewuwoekmcdd.myvnc.com, which at runtime, resolves to 91.148.217.229:13000 (Saudi Telecom DSL Pool).

SHA1: 62b018b011c563dc79831873f780f0abb5e9ecd3  
MD5: da402e22e036c321410d2ce0ec19876b2  
File Type: PE32 executable for MS Windows (GUI) Intel 80386 32-bit  
Packer: BobSoft Mini Delphi  
Anti-Virus Detection Rate: 4 / 12 detection on January 31st, 2014  
Anti-Virus Label: Trend Micro -- “TSPY_SPATET.BMC”  
Mutex: MSCTF.Shared.MUTEX.AJE  
Mutex: MutexToProtectNamespace

The sample creates multiple processes and modifies obligatory DLL files and registry keys as well as creating the following directories and running Project1.exe.

C:\Program Files\java  
C:\Program Files\java\java  
C:\Program Files\java\java\Project1.exe

This sample shares the same mutex -- MSCTF.Shared.MUTEX.AJE -- as a sample we referenced in an earlier blog on point of sale malware as “POSCardStealer,” but that’s not surprising given that at least 3,971,033 samples use the mutex. The second mutex -- MutexToProtectNamespace -- links this sample to malware observed in 2012 and 2013, specifically sending traffic to the DDNS domain bbroman.myvnc.com, labeled in a separate instance by Ikarus as “Backdoor.Win32.Xtreme,” and in other instances successfully evading antivirus software altogether. At least 29,707 malware samples use the mutex -- MutexToProtectNamespace -- which makes it relatively distinct.

Two additional malware samples sending traffic to fuewuwoekmcdd.myvnc.com include:

SHA1: f85b3feee8c72e229800f804084e644445a19558  
MD5: 8bf9bac313f0d50a43a10f19b11b1ae  
PE32 executable for MS Windows (GUI) Intel 80386 32-bit  
Packer: PECompact v1.10b2  
Anti-Virus Detection Rate: 7 / 12 detection on September 18th, 2013  
Anti-Virus Label: Eset -- “a variant of Win32/Injector.ACJQ trojan”  
Destination Traffic: TCP --> 2.89.241.121:13000 (Saudi Telecom DSL Pool)

SHA1: a55f49caaba4dfdf43239a3b18fa849098ddd032c  
MD5: eae96bcf142f076415956b3496e23c7  
PE32 executable for MS Windows (GUI) Intel 80386 32-bit  
Packer: PECompact v1.10b2  
Anti-Virus Detection Rate: 9 / 12 detection on January 30th, 2014  
Anti-Virus Label: Avira -- “TR/Spy.537088.19”  
Destination Traffic: TCP --> 87.109.254.5:288 (Saudi Telecom DSL Pool)

These two malware samples use the same Java icon, but it’s slightly modified. At least 102 other malware samples use the same icon going back to 2010. During runtime analysis all three of these samples send a SYN packet to fuewuwoekmcdd.myvnc.com (which resolves to different Saudi Telecom dynamic IP addresses at different times) without receiving a reciprocal SYN-ACK reply. Perhaps the threat actor’s DDNS is misconfigured. TRAC proprietary intelligence
reveals a small number of current global victims which may be indicative of an ineffective manual spreading mechanism for this particular Trojan.

The threat actor behind this malware campaign may be Saudi, or the host on the Saudi Telecom network may be compromised, and in a perfect world collaboration between the DDNS provider, law enforcement, and Saudi Telecom would produce a quick determination on the nature of the host and further individual attribution. This is just one example out of hundreds of thousands, and based on the previous malware sample numbers, DDNS is being leveraged for an escalating amount of malicious activities. Yet DDNS also represents a solid choke point for global law enforcement to pursue attribution on a large scale.

Incident Response and Security Architecture groups should seriously consider using DDNS as an IoC category for detection and remediation. If traffic to DDNS domains is not necessary on the network, think about implementing a DNS RPZ (Response Policy Zone) -- which is natively available in BIND 9.8.1 and later -- to detect and/or prevent traffic to the most egregious DDNS domains.

For more on this topic please view the “Dynamic Detection of Malicious DDNS” video below.

Tags: DDNS, dns, security, TRAC

In an effort to keep conversations fresh, Cisco Blogs closes comments after 60 days. Please visit the Cisco Blogs hub page for the latest content.

2 Comments.

1. No-IP February 12, 2014 at 11:26 am
Seth Hanford  **February 12, 2014 at 12:19 pm**

Cisco appreciates your response to this blog post. From the data that we see through Cisco Security Intelligence Operations, it’s clear that the features of dynamic DNS, as described in our post, lend themselves to convenience that is welcome in abusive as well as legitimate circumstances. This issue is not unique to No-IP, but as we demonstrated is a problem that occurs on a wide variety of DDNS providers.

We certainly appreciate the offer to collaborate on this, and we’ll reach out privately to start that conversation.

Seth Hanford  
Manager, Cisco TRAC
How the Shift to Mobility & Location-Based Services is Changing Hospitality & Guest Services.
Brendan O'Brien | 21 May 2014
(0 Comments)
Like 4
Tweet 11

Munawar Hossain | 21 May 2014
(0 Comments)
Like 3
Tweet 11

Cisco Announces Intent to Acquire ThreatGRID
Hilton Romanski | 21 May 2014
(1 Comment)
Like 126
Tweet 179

More Posts >
Legal Disclaimer

Some of the individuals posting to this site, including the moderators, work for Cisco Systems. Opinions expressed here and in any corresponding comments are the personal opinions of the original authors, not of Cisco. The content is provided for informational purposes only and is not meant to be an endorsement or representation by Cisco or any other party. This site is available to the public. No information you consider confidential should be posted to this site. By posting you agree to be solely responsible for the content of all information you contribute, link to, or otherwise upload to the Website and release Cisco from any liability related to your use of the Website. You also grant to Cisco a worldwide, perpetual, irrevocable, royalty-free and fully-paid, transferable (including rights to sublicense) right to exercise all copyright, publicity, and moral rights with respect to any original content you provide. The comments are moderated. Comments will appear as soon as they are approved by the moderator.

Switch to our mobile site
Press Releases

Case 2:14-cv-00987-GMN-GWF   Document 5-34   Filed 06/19/14   Page 1 of 10

(408) 509-0000
admin@noip.com

No-IP Dynamic DNS Now
Integrated Into Buffalo Routers

Featured Articles

No-IP Dynamic DNS Now
Integrated Into Buffalo Routers

http://www.noip.com/blog/2014/02/14/self-replicating-malware-found-linksys-routers/
We would like to address a recent report that was released by Cisco Securities.

The report noted many domains that the Cisco Security Team thought were abusive. We have not received any report from Cisco about any domains, or any supporting information. If Cisco wished to
report abuse, they could have easily contacted our Abuse Team at abuse@no-ip.com.

The blog report measured different aspects of domain abuse. We think a key metric not used by Cisco is how fast an abuse report is handled, once properly reported. No-IP excels at handling abuse, verifying reported claims, and taking swift action. We invite Cisco to give that a try. This approach would have been more proactive than posting a blog about the abuse and not reporting their findings directly to us.

We would like to be on the record to state that at No-IP, we have a very strict abuse policy. Our abuse team is constantly working to keep the No-IP system domains free of spam and malicious activity. We work to achieve this by using filters that block certain words and we scan our network daily for signs of malicious activity. Even with such precautions, our free dynamic DNS service does fall prey to cyberscammers, spammers, and malware distributors.

Heartbleed Bug: What you need to know
(http://www.noip.com/blog/2014/04/11/heartbleed-bug-need-know/)
With millions of customers using the No-IP free dynamic DNS service, our users are relying on millions of other people to do the right thing with their hosts, which unfortunately isn’t always the case.

*How does this happen?*

We are one of the last free dynamic DNS providers in the industry and we currently have over 17 million users worldwide. We provide a valuable service for free, but because of this, it is common for users to abuse our service. Our abuse team is amazing and they are usually pretty quick to shut them down, but sometimes a few can slip through the cracks.

Dynamic DNS is often blamed for security issues, but there is so much more to dynamic DNS than just the dark side of it.

Dynamic DNS allows users to access their computer remotely while they are away from the office or on vacation, dynamic DNS also makes it easy for someone to be sure their home or office are safe by monitoring an IP camera remotely, or even check in on their dog while they are away from work. When used correctly, dynamic DNS can make your life easier and safer. Many businesses and Fortune 500 companies even support us in their hardware and recommend our services to their customers.

**Tags**

- [Antispam](http://www.noip.com/Blog/Tag/Antispam/)
- [A Record](http://www.noip.com/Blog/Tag/ARecord/)
- [Backup Mx](http://www.noip.com/Blog/Tag/BackupMx/)
- [Built In Support](http://www.noip.com/Blog/Tag/BuiltInSupport/)
- [Ddns](http://www.noip.com/Blog/Tag/Ddns/)
- [Ddns Client](http://www.noip.com/Blog/Tag/DdnsClient/)
- [Dns](http://www.noip.com/Blog/Tag/Dns/)
- [Domain](http://www.noip.com/Blog/Tag/Domain/)
- [Domain Name](http://www.noip.com/Blog/Tag/DomainName/)
- [Domain Registration](http://www.noip.com/Blog/Tag/DomainRegistration/)
- [Domains](http://www.noip.com/Blog/Tag/Domains/)
- [Dynamic Dns](http://www.noip.com/Blog/Tag/DynamicDns/)
- [Dynamic Ip](http://www.noip.com/Blog/Tag/DynamicIp/)
- [Dynamic Ip Address](http://www.noip.com/Blog/Tag/DynamicIpAddress/)
- [Ecommerce](http://www.noip.com/Blog/Tag/Ecommerce/)
- [Email](http://www.noip.com/Blog/Tag/Email/)
- [Email Forwarding](http://www.noip.com/Blog/Tag/EmailForwarding/)
We pride ourselves in the services that we offer and we highly encourage our users and others to let us know if they come across a hostname that isn’t abiding by our Terms of Service (http://www.noip.com/legal/tos), which includes having more than 1 No-IP account, using our domains to host illegal activity, and a laundry list of other things. We encourage you to report a violation of our TOS or any other abuses of our services to abuse@no-ip.com (email: abuse@no-ip.com). At No-IP we take abuse issues very seriously and work with law enforcement daily to ensure that we are doing our part to keep the internet safe.

Leave a Comment.
Tips & Tricks

8 Interesting Facts About Domain Names
(http://www.noip.com/blog/201-facts-about-domain-names/)

9 Easy Ways to Choose a Secure Password
(http://www.noip.com/blog/201-easy-ways-choose-safe-secure-password/)

Authoritative DNS Servers vs. Recursive DNS...
How to Setup Remote Access For...

Snotty Ron Chocolate Cupcake Recipe

3 Ways to Ensure Your Website...

What is Remote Access and How...

http://www.noip.com/blog/2014/02/12/cisco-malware-report/
<table>
<thead>
<tr>
<th>Featured Articles</th>
<th>Press Releases</th>
<th>Get Connected</th>
</tr>
</thead>
<tbody>
<tr>
<td>No-IP Dynamic DNS Now</td>
<td>No-IP Dynamic DNS Now</td>
<td></td>
</tr>
<tr>
<td>Integrated Into Buffalo Routers</td>
<td>Integrated Into…</td>
<td></td>
</tr>
<tr>
<td><a href="http://www.noip.com/blog/2014/06/05/dynamic-dns-now-integrated-buffalo-routers/">http://www.noip.com/blog/2014/06/05/dynamic-dns-now-integrated-buffalo-routers/</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>What makes No-IP’s Free Dynamic DNS different?</td>
<td>International Payments!</td>
<td></td>
</tr>
<tr>
<td><a href="http://www.noip.com/blog/2014/05/08/what-makes-no-ip-free-dynamic-dns-different/">http://www.noip.com/blog/2014/05/08/what-makes-no-ip-free-dynamic-dns-different/</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FCC Battle Could Change the Internet As We Know It</td>
<td>No-IP Now Has Over 18 million…</td>
<td></td>
</tr>
<tr>
<td>We Are Now Accepting International Payments!</td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="http://www.noip.com/blog/2014/03/20/ip-neutrality/">http://www.noip.com/blog/2014/03/20/ip-neutrality/</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>We Are Now Accepting</td>
<td>No-IP Now Accepts Bitcoin!</td>
<td></td>
</tr>
<tr>
<td><a href="http://www.noip.com/blog/2014/05/08/accept-local-ip-free-dynamic-dns-different/">http://www.noip.com/blog/2014/05/08/accept-local-ip-free-dynamic-dns-different/</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="http://www.noip.com/blog/2014/05/08/accepts-bitcoin/">http://www.noip.com/blog/2014/05/08/accepts-bitcoin/</a></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Cisco Dynamic DNS
Malware Report

(http://www.noip.com/blog/2014/02/12/cisco-malware-report/)

No-IP, World’s Largest Dynamic DNS Provider...

(http://www.noip.com/blog/2014/01/10/noip-strengthens-managed-dns-network/)

Across the...

(http://www.noip.com/blog/2014/01/07/ip-will-attending-ces-2014/)

Home (/) · DNS (/managed-dns) · Mail (/managed-mail) · Support (/support/) · Blog (/blog/) · Sign Up (/newUser.php)