



Bitcoin Domains

Robert McArdle and
David Sancho

Forward-Looking Threat Research Team

Contents

Introduction.....	3
What Is an ADR?.....	4
. <i>Bit</i> Weaknesses for Attackers.....	7
Case Study: A . <i>Bit</i> Trojan.....	9
Conclusion.....	14
References.....	14
Appendix.....	15
Opusattheend.bit.....	15
Bitshara.bit.....	17
Megashara.bit.....	17
Supermegacool.bit.....	18

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

Introduction

Why would something as ordinary as a new kind of top-level domain (TLD) name interest anybody today? Is the level of attention it may receive, especially from security industry observers, even warranted? In the case of *.bit*, we believe it is.

When the Internet was formalized, a few organizations were tasked to keep things in order. The Internet Assigned Numbers Authority (IANA), for instance, was formed to oversee IP space allocation.¹ For domain names, the Network Information Center (NIC) was initially tasked to regulate TLD registrations for domains including but not limited to generic ones such as *.edu*, *.mil*, and *.int*, as well as big ones such as *.gov*, *.org*, *.net*, and *.com*.² A lot more TLDs have now been added to the NIC's list.

In 1998, the responsibility of overseeing Internet domain names was handed to a new entity—the Internet Corporation for Assigned Names and Numbers (ICANN).³ The controls and strict policies that ICANN has over this area have been the subject of complaints among certain cybercitizen groups. ICANN's strict domain creation policies have caused many groups to want to create new TLDs. Over the last couple of years, alternative TLD systems have appeared, so-called “alternative DNS roots (ADRs).” An organization called “OpenNIC” has, for instance, set up a whole new set of parallel TLDs such as *.bbs*, *.geek*, and *.micro*.⁴ It is, however, difficult to categorize exactly what the sites under these domains are. Although they are not invisible because their IP addresses are accessible on the regular Internet, users whose computers are set up to work with standard ICANN domain roots cannot directly access them. Prospective visitors need to use special Domain Name System (DNS) configurations to access ADR TLDs. To more know about other nonstandard ways to obtain information on the Internet, read “Deepweb and Cybercrime: It's Not All About TOR.”⁵

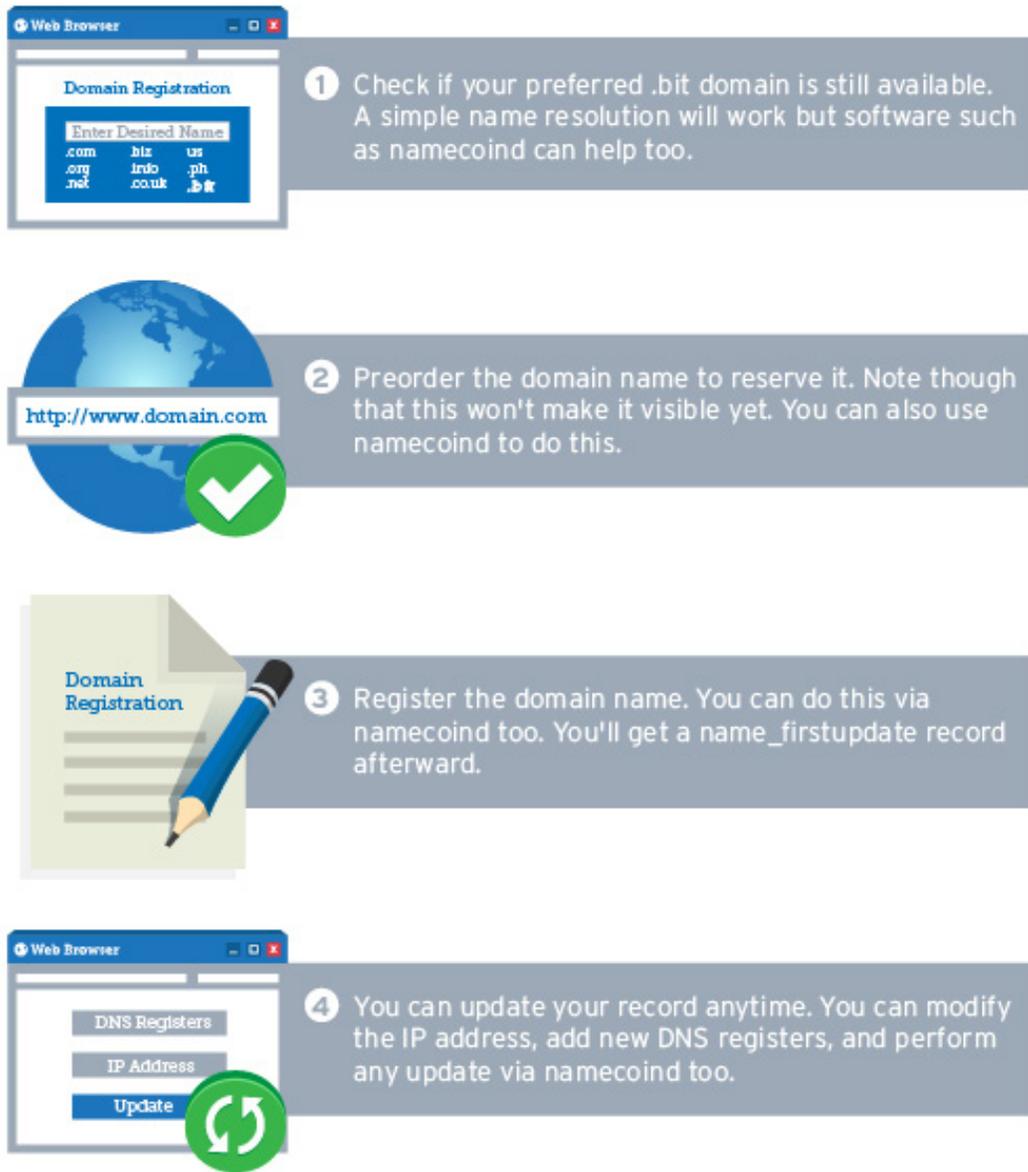
1 Internet Corporation for Assigned Names and Numbers (ICANN). (2013). *IANA (Internet Assigned Numbers Authority)*. Last accessed November 12, 2013, <http://www.iana.org/>.

2 *Nic.com*. (2013). Last accessed November 12, 2013, <http://nic.com/>.

3 Internet Corporation for Assigned Names and Numbers. (2013). *ICANN*. Last accessed November 12, 2013, <http://www.icann.org/>.

4 OpenNIC. (2013). *OpenNIC Project*. Last accessed November 12, 2013, <http://www.opennicproject.org/>.

5 Vincenzo Ciancaglini, Marco Balduzzi, Max Goncharov, and Robert McArdle. (2013). “Deepweb and Cybercrime: It's Not All About TOR.” Last accessed November 12, 2013, <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-deepweb-and-cybercrime.pdf>.



*Or you can opt to use a registration service. Doing so causes you to lose some privacy since you're giving out personal data to a third-party—the registrar

Figure 1: How Namecoin transactions work

Since anyone can create a rogue TLD, it is not surprising that other providers have jumped onto the bandwagon and invented more creative domains. Of special importance to the security community is the *.bit* TLD, designed with a similar philosophy to that of the Bitcoin currency.⁶ *.Bit* domains are paid for with a Bitcoin-clone currency dubbed “Namecoin.”⁷ Not only are these domains extremely inexpensive, they are also completely untraceable, private, and sinkhole-proof. Untraceability and privacy hide the names of the owners of Internet resources from investigators and being sinkhole-proof prevents authorities from seizing malicious domain names. These three qualities are clearly important to certain groups such as cybercriminals.

This paper will attempt to explain what ADR TLDs are and describe the current scope of *.bit* domains, enumerate *.bit* domains’ weaknesses, and present a case study of a *.bit* Trojan and prospective malicious uses of *.bit* domains.

What Is an ADR?

The essence of having an ADR is that someone somewhere can create a new database of domains under an arbitrary TLD. But for clients to successfully resolve domains under such a TLD, they will need to know who to ask first. That is where alternative associations like OpenNIC can help by keeping an index of external DNS servers that allow clients to understand who has the capability to perform the name resolution for a particular ADR.

The *.bit* TLD is based on the Bitcoin philosophy, particularly on a very similar virtual currency, Namecoin. The Bitcoin philosophy refers to the kind of decentralized cohesive collective database that Bitcoin promotes with every separate transaction. In the same way that every Bitcoin user has access to a complete account of every transaction that ever occurred, Namecoin users also have a complete account of all related domains that were purchased and modified from the very beginning. Users have wallets containing Namecoins, which can be mined in a process very much like Bitcoin mining.⁸ In fact, both currencies can be mined at the same time as part of a process called “merged mining.”⁹ As with Bitcoin use, every transaction is recorded in a log called a “block chain.”¹⁰ This log lists every new block as it is mined and every Namecoin sent to other people’s wallets. As of November 9, 2013, 144,830 Namecoin blocks have been mined and 2,537,344 Namecoin transactions have been made. These are not insignificant numbers but still nowhere near the number of Bitcoin transactions made at the same time—26,297,411.

6 Bitcoin Project. (2013). *Bitcoin*. Last accessed November 12, 2013, <http://bitcoin.org/en/>.

7 *Namecoin*. (2013). Last accessed November 12, 2013, <http://namecoin.info/>.

8 Abigail Pichel. (2013). *Threat Encyclopedia*. “Cybercriminals Unleash Bitcoin-Mining Malware.” Last accessed November 12, 2013, <http://about-threats.trendmicro.com/us/webattack/93/Cybercriminals+Unleash+BitcoinMining+Malware>.

9 *Bitparking Bitcoin Merged Mining Pool*. (2013). Last accessed November 12, 2013, <http://mmpool.bitparking.com/pool>.

10 *Blockchain*. (2013). Last accessed November 12, 2013, <http://blockchain.info/>.

In the Namecoin system, each transaction has a field that holds DNS data. For instance, a new transaction from wallet A to wallet B may include the creation of a new domain such as *blah.bit*. The block chain is where DNS servers record every transaction that has ever taken place, which makes it possible to ascertain the current status of the whole *.bit* TLD. A handful of these DNS servers exist, all of which are maintained by Namecoin enthusiasts.¹¹

List of DNS Servers Namecoin Enthusiasts Maintain as of November 9, 2013			
Location	IP Address	<i>.bit</i>	<i>.42</i>
France	88.190.58.119	Yes	No
France	178.32.31.41	Yes	Yes
Netherlands	81.169.248.220	Yes	No
Netherlands	95.211.195.245	Yes	No
Germany	188.40.54.140	Yes	No
Germany	178.63.16.21	Yes	No
Australia	113.20.6.2	Yes	No
Australia	113.20.8.17	Yes	No

As a side note, another TLD that has strong security implications and is worth mentioning is *.42*. The *.42* TLD is an ADR that allows the registration of domains that end with a numerical value. The organization behind the *.42* TLD does not allow the registration of a numerical first-level domain, otherwise situations wherein the domain, *192.168.1.42*, actually resolves to IP address, *1.2.3.4*, can occur. Nothing is, however, stopping others from setting up another numerical ADR TLD that allows such a behavior. This could be very confusing for users and security systems alike.

¹¹ *.Bit Project*. (2013). Last accessed November 12, 2013, http://dot-bit.org/mediawiki/index.php?title=How_To_Browse_Bit_Domains&oldid=1840.

To insert a new entry to the peer-to-peer (P2P) network, a client needs to enter certain information such as the domain being acquired and/or the IP address associated with it. The client then makes a Namecoin transaction wherein the Namecoin gets spent without any particular recipient. This makes the process of getting a new *.bit* domain completely private. There is no need to share personal data or even to provide fake data, as is commonly the case when criminals register Whois details.

To register *.bit* domains, the only requirement is running the appropriate free open-source software on an Internet-connected PC. It is also possible to use third-party registration services although this may diminish the privacy that the Namecoin system provides.

Namecoin payments are as untraceable as Bitcoin payments and what little can be traced can only lead to a given Namecoin wallet, a completely anonymous hexadecimal character string. Unless one publicly posts his/her wallet ID somewhere, it will be very difficult to link such information to a real person. This, along with anonymity due to lack of Whois data, can be a valuable asset to cybercriminals and other malware authors. In addition, the domains are outside any organization's authority so no Computer Emergency Response Teams (CERTs) or law enforcement agencies can bring them down, redirect them, sinkhole them, cancel them, seize them, or do anything to them. Creating, renewing, or modifying a given *.bit* domain cannot be done by anyone other than the original owner the same way that no one can make Bitcoin transactions in the name of another user without having access to his/her wallet.

Another positive effect of using such a naming system, at least for cybercriminals, is that researchers and security professionals cannot contact the IP addresses of the command-and-control (C&C) servers unless they also modify their DNS settings. This means that systems and analysts trying to follow *.bit* links would not be able to generate any traffic to study communications unless their systems were properly configured. Reputation systems would not be able to verify if a site was malicious, as it would look offline to them and so on. This is not necessarily the case when a malware file is sandboxed and alters the DNS settings of an infected system; but in other cases, this will cause issues.

At present, over 106,000 *.bit* domains have been registered.

.Bit Weaknesses for Attackers

The most obvious weakness of using an ADR system is the need to change an infected system's DNS settings in order to access non-ICANN TLDs such as *.bit*. This may be easily detected and corrected by an administrator. In such a situation, it would disable the whole network functionality of the piece of malware even if it were still running on a system. In this respect, utilizing a new DNS server would be an additional failure point for a malware pointing to a *.bit* domain.

The malware's reliance on a third-party DNS server may be a weak point as well. These DNS servers are usually maintained by volunteers, not professionals, and so may go offline or become temporarily unavailable at any time. This is not a concern when using real NIC root servers. Malware authors can, however, try to alleviate this problem somewhat by running reliable DNS servers from bulletproof hosting providers.

The DNS resolution can also be pointed to a *.bit* server without altering the DNS settings of an infected system. An undocumented feature in the Windows® application programming interface (API) allows programmers to specify which DNS servers are going to resolve each specific request. A smart malware author would probably use this system instead of exposing himself/herself by changing a system's settings. It is also worth pointing out that any corporate network can be capable of monitoring where DNS resolutions point to and alert or block those that try to use noncorporate DNS servers.

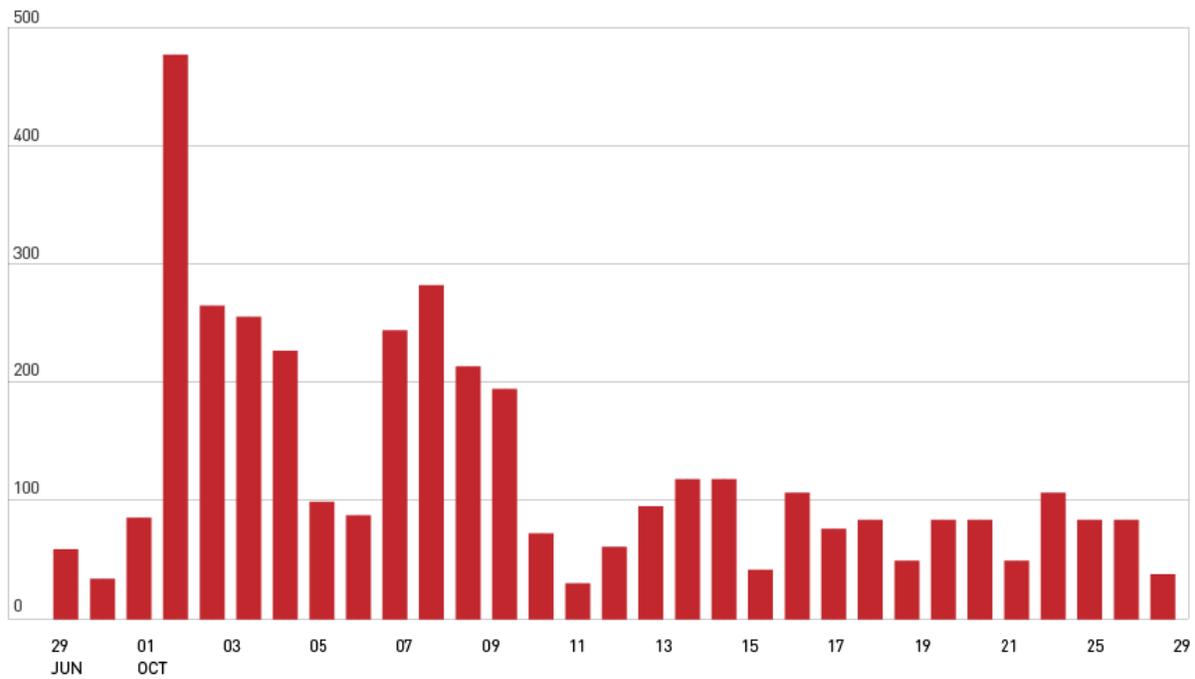


Figure 2: *.bit* access volume per day for a one-month period

Based on the traffic seen, *.bit* domains were not significantly used. Figure 2 shows how small the number of requests per day is to a given *.bit* domain. As shown, most of the requests made were for *opusattheend.bit* and *megashara.bit*. Requests made to other domains were insignificant during this time frame. Spikes in the graphs may be related to specific malware campaigns but the overall numbers are so low that it is easy for variations to occur for minor reasons.

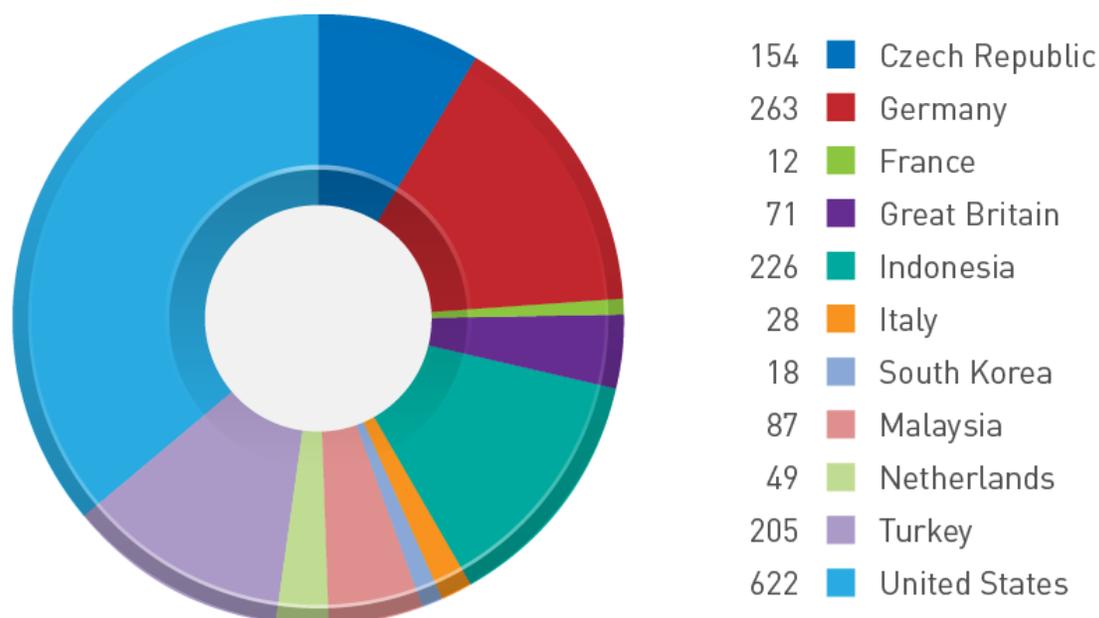


Figure 3: *.Bit* access volume per day for a one-month period by country

Case Study: A *.Bit* Trojan

The Trend Micro™ Smart Protection Network™, a cloud security infrastructure that rapidly and accurately identifies new threats and delivers global threat intelligence to secure data wherever it resides, detected a botnet that operates with *.bit* domains. It is an interesting case with a very unique history. The following *.bit* domains were repeatedly queried:

- megashara.bit
- supermegacool.bit
- bitshara.bit
- opusattheend.bit

The traffic to these four domains was not particularly high. The following table shows the traffic for each *.bit* TLD per day.

.Bit TLD Daily Traffic	
Domain	Number of Hits
Megashara.bit	2,813
Bitshara.bit	857
Opusattheend.bit	164
Supermegacool.bit	2

Many traces to malicious files that accessed some of the given domains as part of their C&C routine, primarily Megashara, Bitshara, and Opusattheend, were seen.

.Bit domains have one additional major weakness. While it is hard for an investigator to discover who is behind a .bit domain, connecting different domains to the same criminal actor is much easier. To illustrate the fact that .bit domains are tremendously easy to map out, we show one such investigation below. This is related to a domain that hosted one of the C&C servers of a particular botnet, *opusattheend.bit*. Since the Namecoin block chain contains every single transaction ever made, including all of the DNS data, we were able to find all of the IP addresses related to a given .bit domain. This kind of historical data is impossible to obtain for normal domains.

The screenshot below shows that *opusattheend.bit* was created on October 29, 2012 and has been updated four times. For example, the last time the IP address of the domain was changed to *213.239.218.69* was on January 28, 2013.

Namecoin block explorer [\[explorer.bit\]](#) [\[testnet.explorer.bit\]](#)

You can search by names, transaction, block id and hash, address

Name : d/opusattheend

Link : <http://explorer.dot-bit.org/n/68941>

Date	Op	Block	Transaction	Value
28/01/13 10:28:41	OP_NAME_UPDATE	93705	2153484	{"ip":"213.239.218.69"}
10/01/13 17:38:43	OP_NAME_UPDATE	91044	2146189	{"ip":"217.23.8.117"}
13/12/12 14:21:13	OP_NAME_UPDATE	87173	2132307	{"ip":["217.172.178.108","94.75.255.65"]}
29/10/12 16:17:32	OP_NAME_FIRSTUPDATE	81422	2072327	{"ip":["62.75.204.20","85.25.151.121","217.172.178.108"]}
29/10/12 13:16:15	OP_NAME_NEW	81406	2072284	Hash : e4557244db00038506775f8033df806653442f90

Figure 4: IP history of *opusattheend.bit*

From a network forensics point of view, this is great information that allows us to see the bigger picture for each *.bit* domain. Since *opusattheend.bit* had all of those IP addresses at some point, “normal” domains that have been pointing to them or which have been moved at the same time to the same servers can be determined and the *.bit* world can then be connected to the ICANN namespace. Subsequently, checking the Whois details on the non-*.bit* domains would uncover the criminal behind them. This is exactly the sort of mistake caused by simple human nature that can often be the undoing of an otherwise careful cybercriminal gang.

Compiling a number of malware hashes that produce or in the past have produced traffic to the four domains could uncover that some samples changed a system’s DNS settings so that every single DNS resolution goes to a *.bit* DNS server. Others may only resolve the *.bit* domains against that server but keep a system’s configuration but all other DNS resolutions. This is probably an evolution of the associated malware family. All malware samples were very similar and detected by the majority of antivirus companies as part of the Necurs family.¹² These were also related to the Virut malware family.¹³

Virut is an old malware family that has been in operation since at least 2006. The very recent Necurs samples, meanwhile, not only connected to *.bit* domains but also include a domain generation algorithm (DGA) routine for added resilience versus takedowns. The Necurs malware family has recently been severely hampered by takedowns by Naukowa i Akademicka Sieć Komputerowa (NASK), the Polish CERT, and other authorities. They were able to sinkhole almost the whole Virut botnet in a way that made the original bot masters lose control of it. As a result, the bot masters have been adding new safety measures to recover the botnet in case takedowns occur again. This has likely led to the new DGA feature and the new experiment with *.bit* domains.

12 Trend Micro Incorporated. (2013). *Threat Encyclopedia*. “NECURS.” Last accessed November 12, 2013, <http://about-threats.trendmicro.com/Search.aspx?language=en&p=necurs>.

13 Trend Micro Incorporated. (2013). *Threat Encyclopedia*. “VIRUT.” Last accessed November 12, 2013, <http://about-threats.trendmicro.com/Search.aspx?language=en&p=virut>.

Conclusion

Non-*.bit* ADRs initially appear to have obvious advantages for future malware campaigns. However, closer reflection quickly shows that other ADRs have the exact same disadvantages as *.bit* TLDs without any real additional advantage. We do not believe a significant number of malware will use ADRs except maybe for political purposes (e.g., avoiding ICANN or making use of ADR TLDs related to a disputed territory such as Tibet—*.ti*).

But since a malware author can use a nonstandard organization to host the TLD, a law enforcement agency or an emergency response team may not have the right contacts to have the offending domain blocked, taken down, or sink-holed. This may ultimately delay law enforcement but not impede it as in *.bit's* case.

On the other hand, for all their advantages when it comes to anonymity and resistance to sinkholing, the fact that *.bit* root servers are not being hosted on professional servers may mean the whole setup can be manipulated by law enforcement agencies. Since the whole system relies on having available and stable DNS servers at all times, this can be the weakest link even though Namecoin exchanges can still normally continue to occur.

To defend against malicious ADR use, an organization needs to evaluate whether it has real need for employees to access non-ICANN TLDs. In most cases, it will not find a real need for such access in a corporate environment. If this is the case, it would be relatively simple to block DNS requests going to external DNS servers. In most situations, only corporate servers should be accessed from within the corporate network. Remote workers accessing from VPNs may need specific policies while connected to a network but may be unprotected while they are not.

Overall, while the setup of the Namecoin system lends itself to an interesting area of study and also initially looked tailor-made for criminal activity due to the disadvantages detailed in this paper, we do not expect to see it achieve mass adoption among cybercriminals for hosting their services.

References

- Abigail Pichel. (2013). *Threat Encyclopedia*. “Cybercriminals Unleash Bitcoin-Mining Malware.” Last accessed November 12, 2013, <http://about-threats.trendmicro.com/us/webattack/93/Cybercriminals+Unleash+BitcoinMining+Malware>.
- Bitcoin Project. (2013). *Bitcoin*. Last accessed November 12, 2013, <http://bitcoin.org/en/>.
- *Bitparking Bitcoin Merged Mining Pool*. (2013). Last accessed November 12, 2013, <http://mmpool.bitparking.com/pool>.

- *.Bit Project*. (2013). Last accessed November 12, 2013, http://dot-bit.org/mediawiki/index.php?title=How_To_Browse_Bit_Domains&oldid=1840.
- *Blockchain*. (2013). Last accessed November 12, 2013, <http://blockchain.info/>.
- Internet Corporation for Assigned Names and Numbers. (2013). *ICANN*. Last accessed November 12, 2013, <http://www.icann.org/>.
- Internet Corporation for Assigned Names and Numbers (ICANN). (2013). *IANA (Internet Assigned Numbers Authority)*. Last accessed November 12, 2013, <http://www.iana.org/>.
- *Namecoin*. (2013). Last accessed November 12, 2013, <http://namecoin.info/>.
- *Nic.com*. (2013). Last accessed November 12, 2013, <http://nic.com/>.
- OpenNIC. (2013). *OpenNIC Project*. Last accessed November 12, 2013, <http://www.opennicproject.org/>.
- Trend Micro Incorporated. (2013). *Threat Encyclopedia*. “NECURS.” Last accessed November 12, 2013, <http://about-threats.trendmicro.com/Search.aspx?language=en&p=necurs>.
- Trend Micro Incorporated. (2013). *Threat Encyclopedia*. “VIRUT.” Last accessed November 12, 2013, <http://about-threats.trendmicro.com/Search.aspx?language=en&p=virut>.
- Vincenzo Ciancaglini, Marco Balduzzi, Max Goncharov, and Robert McArdle. (2013). “Deepweb and Cybercrime: It’s Not All About TOR.” Last accessed November 12, 2013, <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-deepweb-and-cybercrime.pdf>.

Appendix

Opusattheend.bit

- SHA256: 26aaeed6ade8768e91107dc18d43fb6043e8ca45431b2f6df913a4ff93f0e1b9 (this sample connects to *.bit* DNS, *95.211.195.245*)
- SHA256: 1ad1bb6c0f19b1e501e3bc03b44e318dafbb9c9c5cfdb2dc6f9d5fec88d9e525 (this sample connects to *.bit* DNS, *106.187.47.17*)
- SHA256: f5c0d82e1be47d53804e7cd421217a1baa258facf0e2abf316f42fe8ac806517 (this sample connects to *.bit* DNS, *94.231.81.244*)

- SHA256: b1e6f0cad0ae5c60e9e4fa18fd3b4a045d6db172c10a1c8e054e22d1aff4c673 (this sample connects to *.bit* DNS, 94.231.81.244)
- SHA256: 0bcff889dc85df787f65ee6a48da2ba378513a48429903b019f275e277b6dfb6 (this sample connects to *.bit* DNS, 94.231.81.244)
- SHA256: b1e6f0cad0ae5c60e9e4fa18fd3b4a045d6db172c10a1c8e054e22d1aff4c673 (this sample connects to *.bit* DNS, 94.231.81.244)
- SHA256: 611fc9fe0a3f868c3fa2d6c8a972061a60bce7e359d616dcddcd5858bf886f93 (this sample connects to *.bit* DNS, 95.211.195.245)
- SHA256: f0f67fa9b26ee8d7abc2d37d8e5097236c92f486260cfa309a49889a3e2728df (this sample connects to *.bit* DNS, 106.187.47.17)
- SHA256: 771fe8c63ef38b9a48d917db6b06904470ceae007e463624e79b326168aa46f0 (this sample connects to *.bit* DNS, 176.58.118.172)
- SHA256: a6d700306b96861987c2a15086ce62712b9d93624531afa0de12531b0e344406 (this sample connects to *.bit* DNS, 95.211.195.245)
- SHA256: ac7403a3c593d81b0dc895d51151877d302da860c1634afbebf128d3e6167f39 (this sample connects to *.bit* DNS, 176.58.118.172)
- SHA256: 4d6bdf76009143c356c8135a66d8a582428ba7acff5386f54f4766c6e23fbde1 (this sample connects to *.bit* DNS, 106.187.47.17)
- SHA256: 172e8528c7b5506e52dc247ff06daa43174784954d977a2e5994d76f0053474d (this sample connects to *.bit* DNS, 95.211.195.245)
- SHA256: 74bfb227c7f75c118884e072e51fe0b0aab8478b255a6470bbe1647b8b4a4acf (this sample connects to *.bit* DNS, 178.32.31.41)
- SHA256: b912d2a36609f0a5b74b58ce9ab2be5f8a9d2c43a93173261febea145964f08d (this sample connects to *.bit* DNS, 176.58.118.172)
- SHA256: a145315ff99204d52e44141d13b2d13baba85be871dcd4255a2fcb1c1dfe6023 (this sample connects to *.bit* DNS, 106.187.47.17)
- SHA256: cc461ea59acc6cf7f86782a07175999cae4b0e48f0e219dc417dd798da5d9440 (this sample connects to *.bit* DNS, 95.211.195.245)

Bitshara.bit

- SHA256: 98fb9778208cb74c11a71afd065ae64e562ded1ae477ad42e392fe3711170319 (all DNS connections lead to *94.231.81.244*)
- SHA256: 1f9a164fcfaabc3280c6511ff8e3d7afd215b5629559456db595640b99fb eaf4 (this sample connects to *.bit* DNS, *94.231.81.244*)
- SHA256: 0cda3e039aa6b92f5cd45416b1ce487a7e2f720e8310c8c32a67e3e4624c9129 (this sample connects to *.bit* DNS, *94.231.81.244*)
- SHA256: 0585fd9f28ec503541959885a2494fa5a8b609d4c0110d45486508078450f512 (all DNS connections lead to *95.211.195.245*)
- SHA256: b48db19d48f56b94209ba93be07d31938825bf9d683c9c41cebea0c2ace74db0 (all DNS connections lead to *106.187.47.17*)
- SHA256: d2d51b6b3d3a2da954519f386d7ee1050d9bfb413a7367eec31ba0bc3569e54 (this sample connects to *.bit* DNS, *95.211.195.245*)
- SHA256: 0585fd9f28ec503541959885a2494fa5a8b609d4c0110d45486508078450f512 (all DNS connections lead to *95.211.195.245*)
- SHA256: 0585fd9f28ec503541959885a2494fa5a8b609d4c0110d45486508078450f512 (all DNS connections lead to *95.211.195.245*)
- SHA256: 47217f5daf5ae922b252ea795789ec0bea13b918686f8d051b58625ab077f4c4 (all DNS connections lead to *94.231.81.244*)

Megashara.bit

- SHA256: 8fd8de86ba98278da8e6dcee65f6a47020dacec75557059cb2a748fa1bea ba05 (all DNS connections lead to *106.187.47.17*)
- SHA256: 2ca7804dbd64ae5855b5387cb5123e22ab06f034a49b93ffcb7f8e85de5 e30ac (all DNS connections lead to *178.32.31.41*)
- SHA256: 4190c7a9078675f81d8f3e9eb8dc7be1fff0f3d7d39106636ac981920383626d (this sample connects to *.bit* DNS, *95.211.195.245*)
- SHA256: 62c73726da2745f4a664c00af860a14cbf4cad5592318087ae922d28b6e1a7b5 (all DNS connections lead to *95.211.195.245*)
- SHA256: 2ca7804dbd64ae5855b5387cb5123e22ab06f034a49b93ffcb7f8e85de5 e30ac (all DNS connections lead to *178.32.31.41*)

- SHA256: cfe6e02e3470b28aa59fcc7a9ec4c3269a3c66c4c15952e506fd7ab43bc4b279 (all DNS connections lead to *95.211.195.245*)
- SHA256: 0ccb749acba256dcd43d92f31fc3473ecd052fed65d5302c73b8b018b5494cae (this sample connects to *.bit* DNS, *106.187.47.17*)
- SHA256: 4190c7a9078675f81d8f3e9eb8dc7be1fff0f3d7d39106636ac981920383626d (this sample connects to *.bit* DNS, *95.211.195.245*)
- SHA256: 0ccb749acba256dcd43d92f31fc3473ecd052fed65d5302c73b8b018b5494cae (this sample connects to *.bit* DNS, *106.187.47.17*)
- SHA256: 8fd8de86ba98278da8e6dcee65f6a47020dacec75557059cb2a748fa1beaba05 (this sample connects to *.bit* DNS, *106.187.47.17*)

Supermegacool.bit

- SHA256: ebbfe2287237837a32e1482edea2c644e879be9b19c0cea9da92b06f3b8cee9c (this sample connects to *.bit* DNS, *106.187.47.17*)
- SHA256: 820a38b1513fd7f7cea36017db8c7b417adffc1f44e43ba3f41e4e5f3bdf1af3 (this sample connects to *.bit* DNS, *106.187.47.17*)
- SHA256: 0b15e190ac720f5d55042525c438c8e63650330b34b490cc08d42d7ef7312b44 (this sample connects to *.bit* DNS, *106.187.47.17*)
- SHA256: 965af2e577b1c9a6c6016fa6e3c39148e531326719724b88b00841def4d82c80 (this sample connects to *.bit* DNS, *106.187.47.17*)
- SHA256: 8cbd5e0cfe81d15874178f36fc4d148cc5f1bab3d913527c6176aea61cf5073d (this sample connects to *.bit* DNS, *178.32.31.41*)
- SHA256: 0b15e190ac720f5d55042525c438c8e63650330b34b490cc08d42d7ef7312b44 (all DNS connections lead to *106.187.47.17*)
- SHA256: ba4ff1b6802934830d091af5699a02c280f7faed3f084ceaffa3421c7623391c (this sample connects to *.bit* DNS, *106.187.47.17*)
- SHA256: 9f3de54a5f57da7e9f95d82268b027768d913a3564995061970174caf63a522e (this sample connects to *.bit* DNS, *106.187.47.17*)
- SHA256: 213d251aa3402a871209530a1af0ce117fd372734d0c2849d1ebfd8dd12d0358 (this sample connects to *.bit* DNS, *95.211.195.245*)

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.

©2013 by Trend Micro, Incorporated. All rights reserved. Trend Micro and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.



10101 N. De Anza Blvd.
Cupertino, CA 95014

U.S. toll free: 1 +800.228.5651
Phone: 1 +408.257.1500
Fax: 1 +408.257.2003

Securing Your Journey
to the Cloud