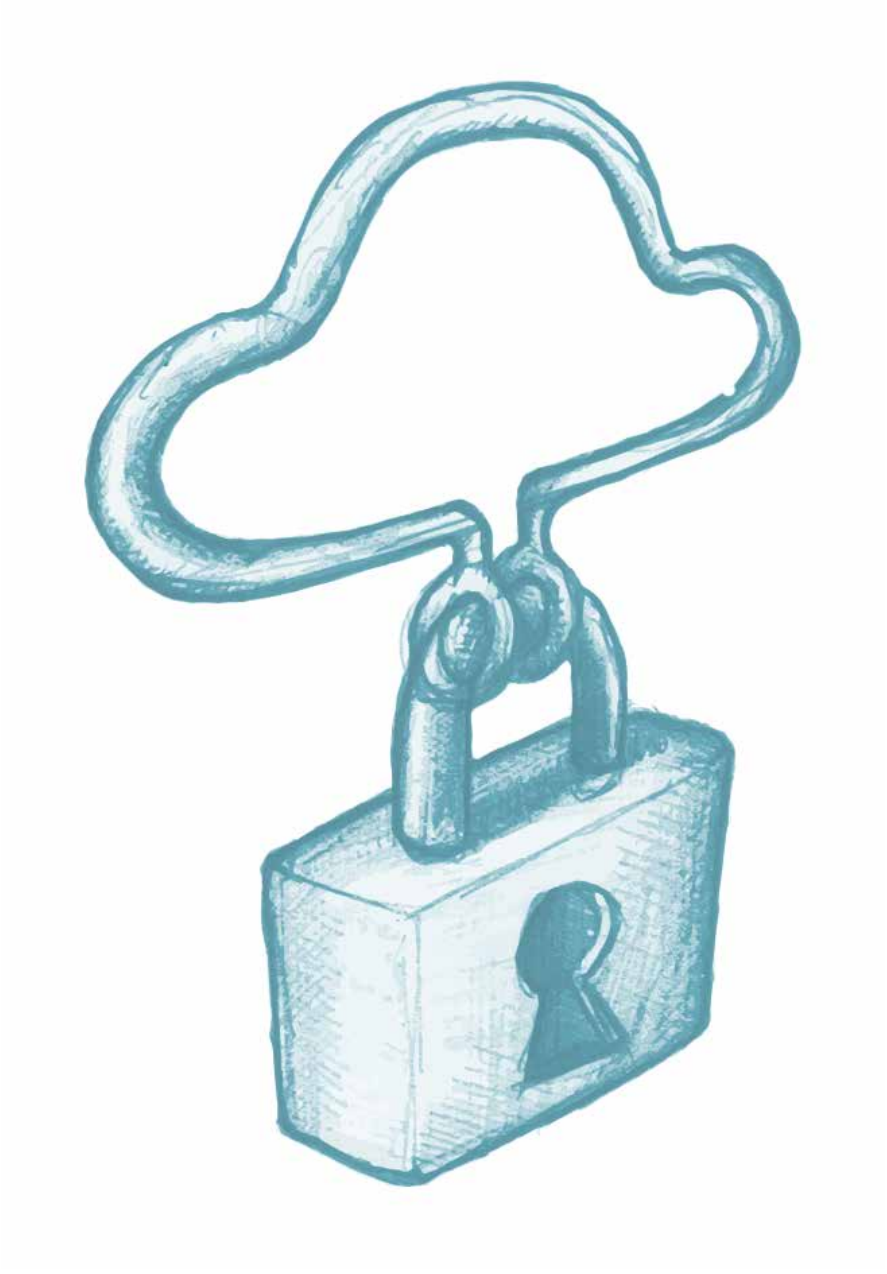
Bitdefender

Security Business Review

Q4: 2014

Bitdefender



By Bitdefender Labs

Botnet Anonymization Raises New Security Concerns

Executive Overview

While botnets, which are large groups of compromised computers managed from a centralized command and control (C&C) system, have been a security concern for many years, they continue to evolve. As security companies and law enforcement have enhanced techniques used to disrupt C&C, criminals continue to improve C&C techniques to avoid such disruptions. Botnets are a resource that criminals sell to send SPAM, perform denial of service (DoS) and distributed denial of service (DDoS) attacks, while they have also been involved in the rise of ransomware incidents. **The Security Business Review** examines some of the latest C&C anonymization techniques found in the wild today.

Botnets are profitable

The accelerating rate at which malware is being pushed into the wild is raising concerns amongst not only security vendors, but also end-users and organizations. Ranging from trivial to highly sophisticated, malware is a challenge for even seasoned security researchers. Detection, removal, and mitigation are significant obstacles posed by advanced threats, and are leveraged as advanced tools by those who orchestrate advanced attacks.

While incidents of denial of service (DoS) and distributed denial of service attacks (DDoS) continue to rise, there are other nefarious uses for botnets. Used as a **commercial malware delivery platform**, leasing a botnet for a short period of time allows the immediate deployment of malware samples (commercial ransomware in particular) that may lead to infection of even more systems.

Denial of service (DoS) and distributed denial of service (DDoS) attacks have increased not because of ideological motivations, but because of **financial motivation**. Likewise, **accessing critical company** data and **selling it to the highest bidder** (or, in the case of ransomware, **selling it back to the owner**) offers far greater financial reward than other cybercriminal activities.

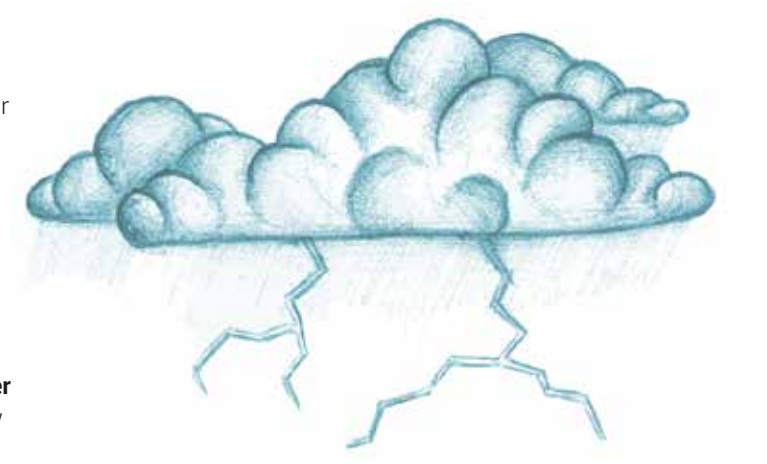
Botnet footprints in enterprises range from botnets that inadvertently infiltrate computers (due to lack of company policies), to enterprise targeting, and state-sponsored attacks. **Enterprise-targeted botnets** usually rely on sophisticated multi-purpose Remote Access Trojans (RAT) with worming functions that are able to exploit standard network services. Usually, they include native proxy support and the capability of using the user's credentials for navigating out of the network, to a Command & Control server.

Other types of botnets rely on **off-the-shelf malware components** (built from **commercial DIY malware kits**). This means that the bot-master has a high degree of knowledge about the enterprise and already knows where to find the valuable information.

State-sponsored tools targeting specific industries and technologies vary in both sophistication and functionality, and don't usually follow any type of discernable pattern when it comes to both infection vectors and payloads.

Bitdefender®

Botnets – the dark cloud



The prevalence of Internet-connected devices makes it easy for a bot-master to seize and control thousands, if not hundreds of thousands, of "zombies". Our own data shows that the vast majority of devices that are currently part of a botnet are located in Asia.

As with any network of endpoints, a degree of control must be maintained. The methods and infrastructure used to control a botnet have evolved significantly. Using **Tor anonymization** to command an entire network of "zombies", along with **multi-tier proxies**, is a new trend that raises serious concerns about how these large infrastructures could be dismantled.

The classic botnet works by dialing back to a relatively static C&C server, making it straightforward for a security company to initiate a takedown and set up a black holing system. Today, we are seeing large botnets that have far more sophisticated C&C methods. Below, we explore **two well-known botnets**, and the **techniques** that they have used.

CryptoLocker Research

When CryptoLocker gains access to a computer, it contacts its command-and-control center, which, in turn, generates a 2048-bit RSA key pair. The public key is sent back to the computer and will be used to encrypt files with specific extensions. To give an idea how strong the key is, imagine that, if one victim would have started cracking the key on a regular computer right after the Big Bang, they would be 0.02% through decryption.

Our own research into Cryptolocker has revealed that the **entire anonymization process is handled via multi-tier proxies that hide the communication between bots and the bot master.**

The Tier-1 proxy server forwards the victim's traffic to a secondary server to anonymize it and hide the location of the key server. This proxy also handles domain name resolution allowing its operators to rapidly perform name changes and avoid suspension.

The Tier-2 proxy server takes the information forwarded by the Tier-1 server, filters it and forwards it via GRE tunnels to other servers (most likely Tier-3 proxies). The server has 10 different IP addresses. When data packets reach the first interface, they are automatically forwarded through a specific GRE tunnel and traffic is prioritized appropriately. When probed from IP addresses belonging to law enforcement, CERTs or security companies, the server implements a mechanism to add them to a black hole, routing all packets from the respective IPs to /dev/null.

The Tier-2 server handles two main functionalities: **it secures traffic by screening** its origin and **blocking law enforcement or security companies**; and it **sends the data received from Tier-1 servers through highly encrypted & redundant connections**.

Note: Both the Tier-1 and Tier-2 proxies can be rapidly customized by deploying specialized tools (belonging to those that developed the ransomware) made available by the owner of the infrastructure. When either of the tools are run, a regular server becomes a Tier-1 or Tier-2 proxy in a matter of minutes, depending on the DNS propagation time.

Although Cryptolocker may be gone thanks to joint efforts of security companies and law enforcement agencies, there is still the issue of the content delivery network. A botnet's backbone is the communication infrastructure, and in this case, it is designed not only to scale operations up and provide redundant access to other nodes in case of failure, but also to anonymize the data flow and prevent victims, law enforcement or security organizations from tracing the real operations center.

The **new generation** of **anonymized botnets** has been designed to be **completely scalable, hidden**, and **extremely flexibl**e when recovering after massive takedowns, all thanks to anonymizing communication via Tor.

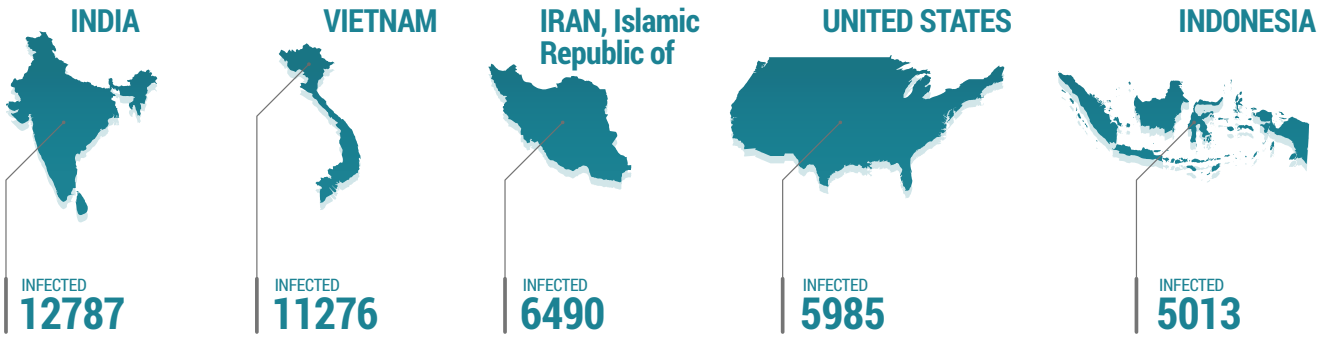
PushDo Research

Pushdo, a spam Trojan and a malware dropper also uses **private** and **public keys** to **protect the communication between the bots and the C&C server**. Primarily used to send spam from infected machines, it can also download other malicious files.

New PushDo binaries contain an **encrypted overlay**, having the **role of a checkup**. If the conditions specified in the overlay aren't met, the sample doesn't run properly. Also, the list containing approximately 100 clean domain names, which hide the hard-coded domain name of the C&C can be found here and not in the binary file.

It also uses a **new DGA (Domain Generation Algorithm)** to generate domain names that are different from previously analyzed samples.

After sinkholing one of them, we found the number of infected machines calling home to the C&C, and ranked them by country. This is the top forty:



Rank	Country	Infected	Rank	Country	Infected
1	India	12787	21	Pakistan	1119
2	Vietnam	11276	22	South Africa	1096
3	Iran, Islamic Republic of	6490	23	Kazakhstan	1065
4	United States	5985	24	Venezuela	1024
5	Indonesia	5013	25	Algeria	1022
6	Thailand	4678	26	Spain	939
7	Turkey	4507	27	China	914
8	Peru	4168	28	United Kingdom	910
9	Argentina	4132	29	Germany	870
10	Mexico	3433	30	Romania	865
11	Egypt	2442	31	Japan	858
12	Italy	2271	32	Morocco	755
13	Philippines	2257	33	Saudi Arabia	750
14	Brazil	1858	34	Chile	737
15	Taiwan	1833	35	Ukraine	724
16	Russian Federation	1602	36	Korea, Republic of	683
17	Malaysia	1586	37	Guatemala	666
18	Poland	1336	38	Ecuador	641
19	France	1214	39	Israel	597
20	Colombia	1213	40	Hong Kong	561

Bitdefender

Final Thoughts

We strongly urge **end-users** to pay **extra attention to the resources they visit online**, as well **what they install on their computers. Software updates for third-party products** such as Java, Adobe Reader and Flash should be **deployed as soon as they become available**, along with operating system updates. **The use of an anti-malware solution is, as always, highly recommended.**

Enterprises likewise need to **maintain patch levels** and **run strong antimalware on all systems. Centralized management** and **highly capable staff** should be considered baselines of protection. Identifying a small cluster of infected systems, perhaps by detecting an 'over-the-counter' piece of malware, may be exactly what it seems. However, it may be that the weakest link in a chain of attack has been discovered, and extra investigation and vigilance is needed to be sure that other parts of the attack do not persist.

Bitdefender

Bitdefender delivers security technology in more than 100 countries through a cutting-edge network of value-added alliances, distributors and reseller partners. Since 2001, Bitdefender has consistently produced market-leading technologies for businesses and consumers and is one of the top security providers in virtualization and cloud technologies. Bitdefender has matched its award-winning technologies with sales alliances and partnerships and has strengthened its global market position through strategic alliances with some of the world's leading virtualization and cloud technology providers.

FOR MORE INFORMATION VISIT: enterprise.bitdefender.com

30102014-Bitdefender-Business-SecurityBiz-A4-en_EN