Operation b70

Nitol Malware Research and Analysis

Microsoft Digital Crimes Unit

Table of Contents

Getting to know Nitol

In August 2011, researchers on the Microsoft Digital Crimes Unit purchased 20 computers from various cities in China. About half of these computers were laptops while the other half were desktop computers. After looking at each of the computers, the researchers found that one of the laptops was infected with the Nitol virus. They also noticed that the virus comes in two variants - .A and .B. Except for minor differences, the variants can be considered equal in terms of their capabilities and functionality. Out of the 20 computers analyzed by DCU's researchers, four contained files detected as malware by antivirus companies. The three computers not infected with the Nitol malware were infected with other types of malware.

Sample Computer	Malware Name	SHA1	Behavior
#10: WinXP SP3	Nitol	99624d63106ccff4a2e2feb9d32437bfd2f183ab	HTTP Backdoor
#11: Win7 SP1	Trafog	a6293ac854ade333a1faa3acabb15dfe777d5bae	FTP Backdoor
#12: WinXP SP3	EggDrop	E4E583E7FA0CF566586D828DB019F2C7291C4F39	Suspicious – non-malicious
#17: Win7 SP1	Malat	37e4be0b473ceba6144fa5b900cae52b4c85c47e	IRC Backdoor

Table 1: Anti-Virus scan results from computers purchased from the Chinese retailers.

The computer that contained the Nitol virus was the only one that was actively running and had attempted to connect to a command and control (C&C) server. Because of this activity, DCU's researchers primarily focused its study on Nitol, looking at its behavior, telemetry, and network behavior following the study. The content below describes and analyzes the harm that the Nitol-infected computers pose to a victim and others.

Infection

Nitol infects users through a variety of common mechanisms, including activities like distributed denial of service (DDOS) attacks. What makes Nitol especially interesting is that it was developed to be spread through removable media (e.g. USB flash drives, external hard drives, zip/rar files, etc.) and mapped network shares. That is, once a computer is infected with the Nitol malware, any piece of removable media that connects to the infected computer will also become infected as the virus if capable of copying itself. These infected USB flash drives, external hard drives, and/or mapped network shares can infect any system or computer it comes into contact with. One thing to note is that Nitol is selective about where it copies itself to the drives. It picks directories that contain applications (.EXE, .DLL, .OCX files) and compressed file archives (e.g. .RAR and .ZIP). The Nitol developers knew this would result in a large number of files being copied to every directory on a drive, so they decided to hide the files with the file attributes SYSTEM/READ-ONLY/HIDDEN. Files with these attributes are considered "super hidden" and are not viewable by Windows Explorer by default.

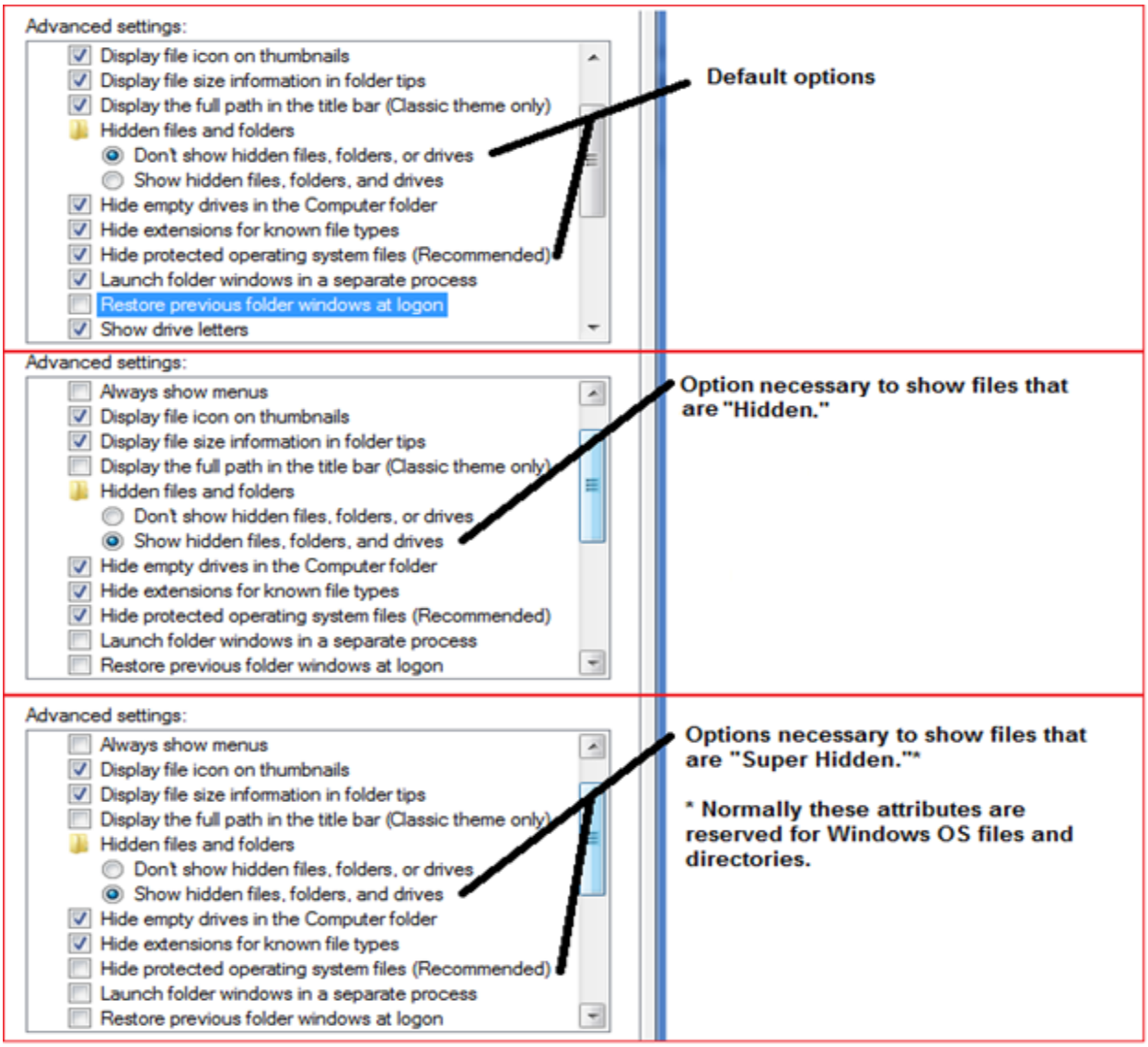


Figure 1: Windows Explorer options: default, show hidden files, and show super hidden files.

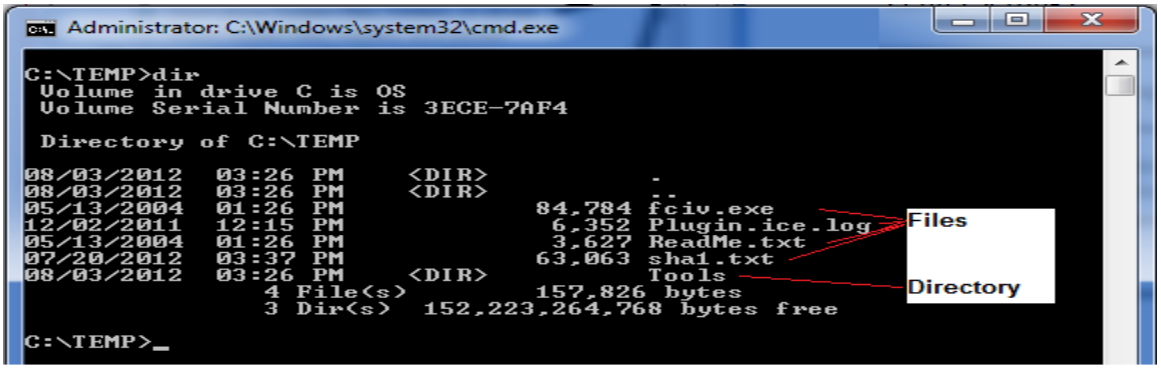


Figure 2: Advanced users may locate files on Windows from within a command prompt by typing the "dir" command. They will never see Hidden or Super Hidden files without issuing the /A option. Alternatively, more advanced users may use the "Attrib" command.

The reason Nitol copies itself to directories containing applications (primarily files with extensions .EXE) is to exploit the module loading process used by Windows when it runs applications.

Applications load several different types of files when they are started (e.g. run, launched, executed, etc.). Some of these files contain code that the application uses. These code-carrying files are called dynamic link libraries and typically have the file extension ".DLL." When an application is started, it is important to note that Windows tries to find the file (on the application's behalf) in the application's directory first. If one is not found, then several other places are searched and then the process ends with a search in the Windows\System32 directory.

Nitol's filename is called LPK.DLL. This file is loaded by all programs that have a user interface and some that do not. Since applications look for LPK.DLL in their current directory before any other place, Nitol will get loaded before the file (of the same name) provided by Microsoft in the System32 directory.

Spreading Nitol is simple to do using this mechanism as a cybercriminal does not need to trick the user into running an application for infection to occur. Instead, the Nitol LPK.DLL file merely needs to get copied to a directory that contains an application the user is likely to use.

After Nitol copies LPK.DLL to a form of removable media, any user that runs an application from that removable media will infect the computer on which they run the application, e.g. laptop, home, work, or public kiosk machine. This also means that Nitol can bridge network boundaries and security mechanisms, because people typically carry Setup programs, application patches, and other software between home and work using removable storage devices. These Setup programs, application patches, and other forms of software being used through removable storage devices are all vulnerable to this infection mechanism.

Below is footage of the system purchased in China that came to us infected with the Nitol virus. The video shows the virus infecting a USB flash drive by copying itself to all of the directories that contain applications. It's important to note that this USB flash drive had several applications stored on it that, when run from other computers, would distribute and spread the infection.

Behavior

To date, all of the versions of the Nitol malware have been rootkits. Some other generic names include backdoors. Microsoft Anti-virus labels them Trojan: Win32/Nitol.A and Trojan: Win32/Nitol.B. Nitol runs as a background process (e.g. hidden application without UI) and performs the commands sent from an attacker. The following list of commands was retrieved by reverse engineering the Nitol.A sample we received in China. This list is the same as the functionality contained within Nitol.B samples obtained by Microsoft Malware Protection Center (MMPC).

C&C Command ID	Action	Threat
0x01 (1)	Receive Component	Send a new module to the computer to run.
0x02 (2)	Unknown but DDOS Specific	• Nitol connects to target address via TCP, UDP, or RAW.

0x03 (3)	Unknown but DDOS Specific	• Possible floods: SYN, TCP, UDP, ICMP, HTTP. • C&C may command sleep for specific time.
0x04 (4)	Unknown but DDOS Specific	
0x05 (5)	Stop Work	Stop DDOS'ing target computers
0x06 (6)	Clean up	Delete, set file attributes to Normal. Exits.
0x10 (16)	Download & Run	• Specify URL and filename to download from Internet • Save file in temp directory under filename "stf[5 random letters].exe" • Executes saved file
0x12 (18)	Update	• Delete existing service • Download new executable from specified URL • Save file in temp directory under filename "stf[5 random letters].exe" • Execute saved file
0x13 (19)	Open URL	Launch Internet Explorer (specifically) with specified URL
0x14 (20)	Open URL as Current User	Launch Internet Explorer (specifically) with specified URL
0x20 (32)	Start Work	Start DDOS'ing target computers

0x77 (119)	Get Computer Information	• Get computer information and send to C&C
		  ○ Computer Local (e.g. EN-US)
		  ○ Computer Name
		  ○ Operating System Name
		  ○ Amount of memory (RAM)
		  ○ CPU Speed
		  ○ Nitol Flag (possibly version number)
		  ○ Nitol Work DLL flag
		  ○ Timestamp

Table 2: Nitol command and control server instructions and descriptions. Yellow denotes DDOS specific commands.

Nitol.x Family

Microsoft Anti-virus started tracking Nitol.A in February 2011. A quick look at the growth rate of infections since this date suggests that the virus' distribution significantly increased in that year. It is important to note that Nitol telemetry data supporting the statistics in this document are sourced from Microsoft Anti-virus, Smart Screen, and Bing/Search teams. The chart below represents a subset of the global infection landscape of this threat.

Variant	**Samples Count**
Nitol.A	1,932
Nitol.B	268
All Variants	*2,200*

Table 3: Unique number of Nitol samples collected by MMPC since February 2011.

The Nitol family started in Asia, most likely China, since this is where early detections originated from. In August 2011, Microsoft's researchers purchased a Windows laptop computer from computer reseller in Shenzhen, China, which had been carelessly or intentionally infected with Nitol.A. This computer was a Hedy laptop installed with Windows XP Service Pack 3. The presence of the Nitol.A infection on this computer concerned Microsoft and also put the malware on the Digital Crimes Unit's radar.

As previously mentioned, DCU's researchers discovered that Nitol has two primary variants, .A and .B., and that these variants have similar functionality and capabilities.

Each Nitol variant has a primary C&C domain or IP address hardcoded into the malware. The diversity of these built-in locations strongly suggests that individuals, rather than large organized gangs, are controlling the infected computers. Since the functionality of the virus makes it capable of doing anything that the attacker wishes it to, DCU's researchers could not use behavioral analysis to create subversions of this malware like they did with Rustock.

Each Nitol variant analyzed by MMPC and DCU has similar functionality. In addition, both contain built-in features to either attack computers on the Internet or to run software of the attacker's choosing. The fact that a DDOS feature is built into the malware strongly suggests that it was initially created to perform this job. The second feature supports the background download and execution of programs. This feature makes Nitol a backdoor, allowing an attacker to take over a victim's computer.

Nitol.B samples analyzed by DCU for network behavior have been seen to perform DDOS attacks. Both Nitol.A and .B variants have been traced to active C&C servers. Analysis suggests that there is no common theme between samples or the action the bots are performing. Most network traffic analyzed thus far shows the bots to be active, but awaiting instructions.

Nitol Infections

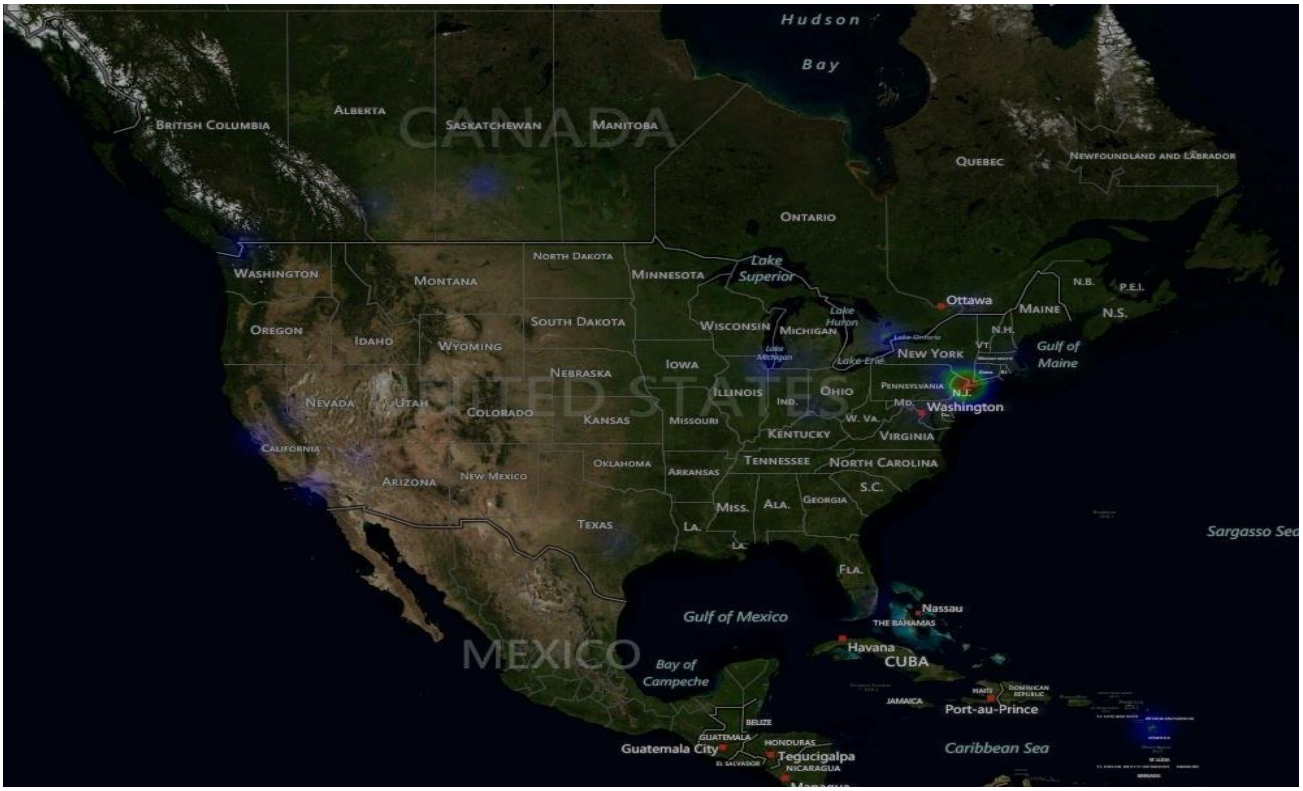
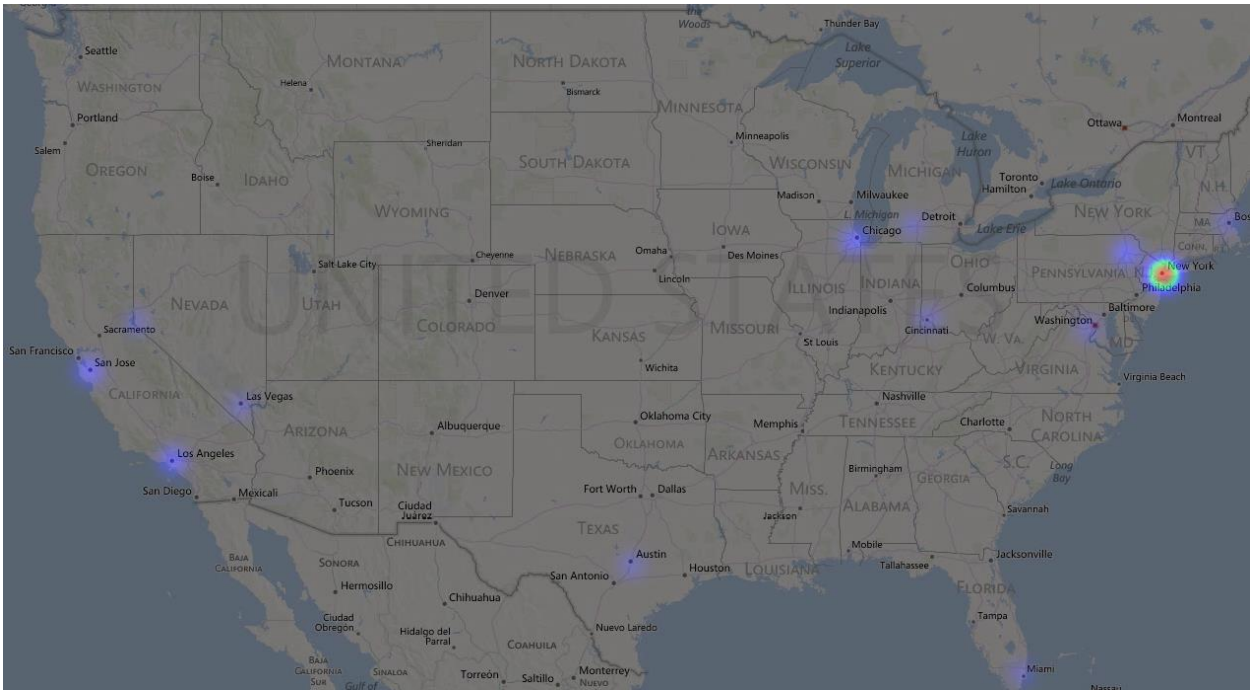


Figure 3: Geographic distribution of computers infected with Nitol.A & .B variants; North-Western Hemisphere (above). Nitol infections concentrated mostly in California, New York, and Pennsylvania (below).


Seattle
Portland
Salem
Boise
Helena
Bismarck
Sheridan
Thunder Bay
Lake Superior
Minneapolis
Ottawa
Montreal
Toronto
Hamilton
Lake Ontario
Madison
Milwaukee
Chicago
Detroit
Lake Erie
Omaha
Des Moines
Cheyenne
Salt Lake City
Denver
Lincoln
Columbus
New York
Philadelphia
Baltimore
Washington
Indianapolis
Cincinnati
St Louis
Wichita
Sacramento
San Francisco
San Jose
Las Vegas
Albuquerque
Oklahoma City
Memphis
Nashville
Charlotte
Virginia Beach
Los Angeles
Phoenix
San Diego
Mexicali
Tucson
Ciudad Juárez
Fort Worth
Dallas
Birmingham
Jackson
Savannah
Austin
San Antonio
Houston
Mobile
Tallahassee
Jacksonville
Hermosillo
Chihuahua
Ciudad Obregón
Hidalgo del Parral
Nuevo Laredo
Tampa
Miami
Torreón
Saltillo
Monterrey
MONTANA
NORTH DAKOTA
MINNESOTA
WASHINGTON
OREGON
IDAHO
SOUTH DAKOTA
WISCONSIN
MICHIGAN
WYOMING
IOWA
NEBRASKA
ILLINOIS
INDIANA
OHIO
PENNSYLVANIA
NEW YORK
NEVADA
UTAH
COLORADO
KANSAS
MISSOURI
KENTUCKY
VIRGINIA
W. VA.
CALIFORNIA
ARIZONA
NEW MEXICO
OKLAHOMA
ARKANSAS
TENNESSEE
NORTH CAROLINA
S.C.
GEORGIA
MISS.
ALABAMA
TEXAS
LOUISIANA
FLORIDA
CHIHUAHUA
SONORA
COAHUILA
BAJA CALIFORNIA
BAJA CALIFORNIA SUR
SINALOA
NUEVO
VT
N.H.
MA
CONN.
MD
Long Bay

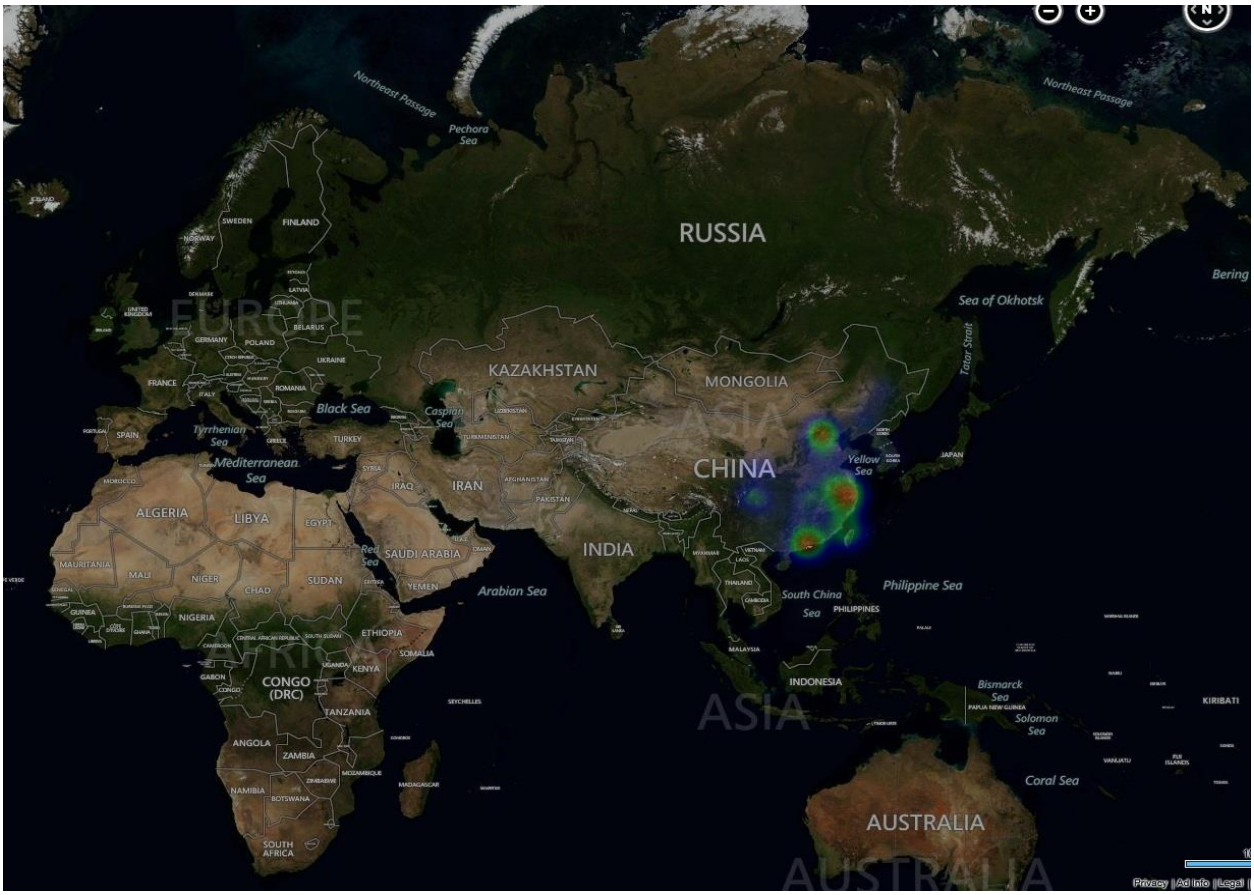


Figure 4: Geographic distribution of computers infected with Nitol.A & .B variants in Eastern Hemisphere (above). Nitol infections concentrated mostly in Guangdong, Beijing, Shanghai, and Taipei (below).

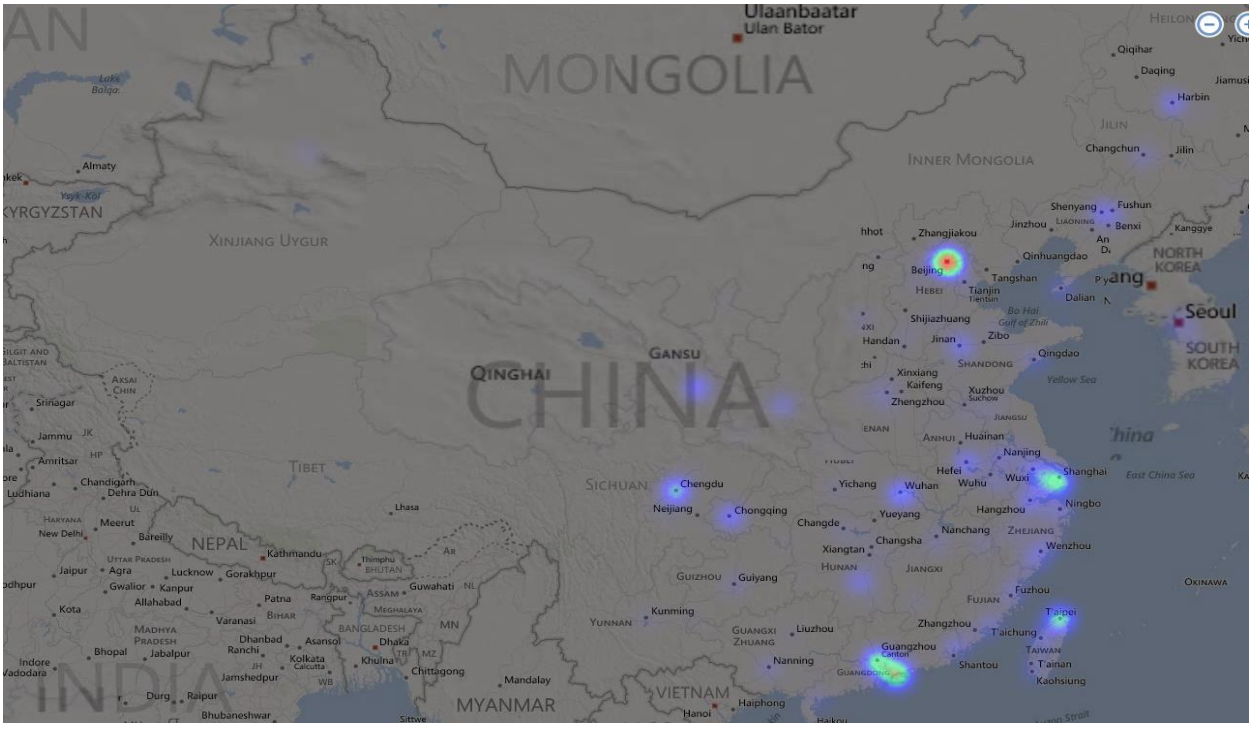


Figure 5: Above is a worldwide map showing the locations of the servers that control customer's computers infected with Nitol.

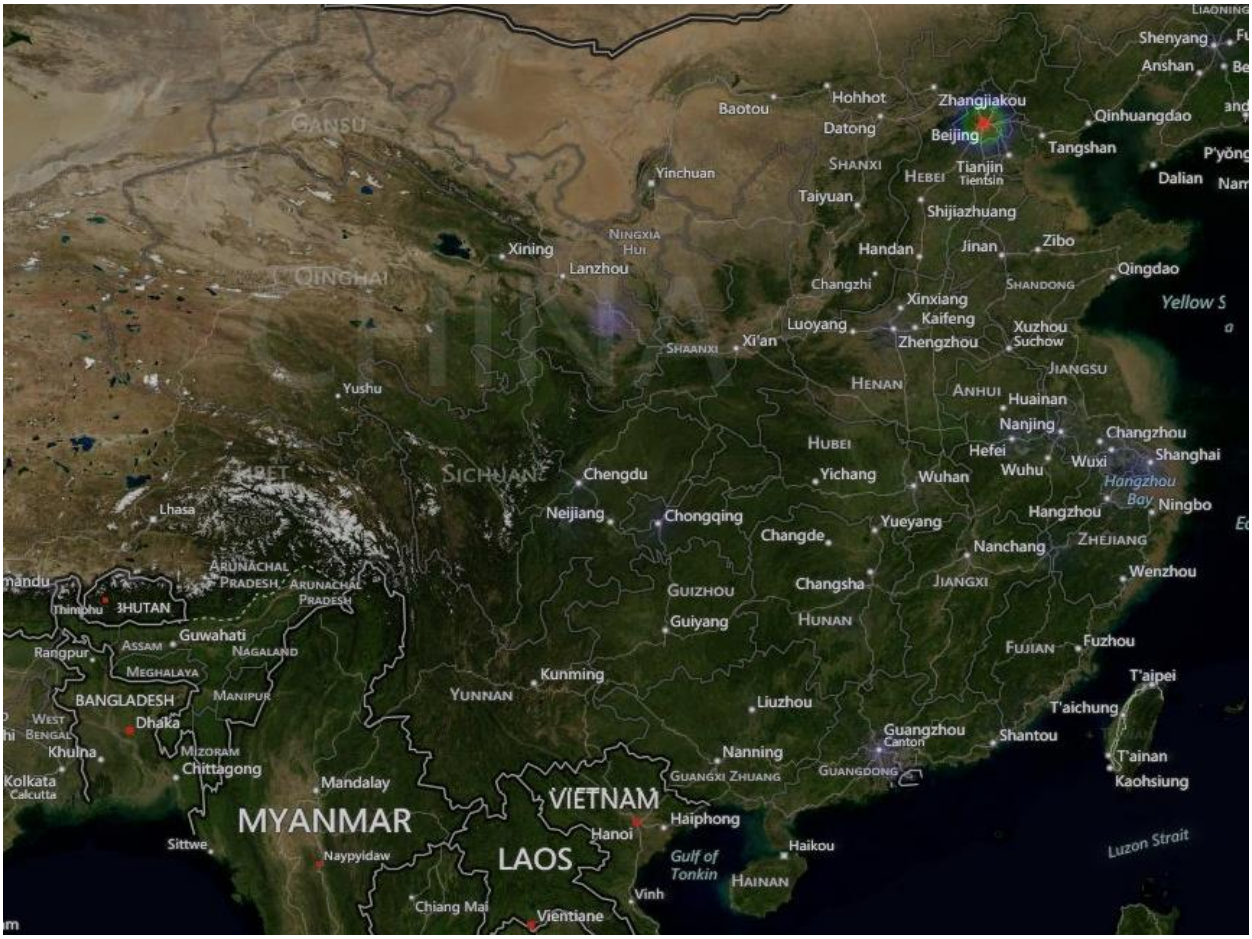


Figure 6: China, by far the largest country with Nitol-controlling servers, does so mainly from Beijing. China tops the list of countries that send commands to infected computers.

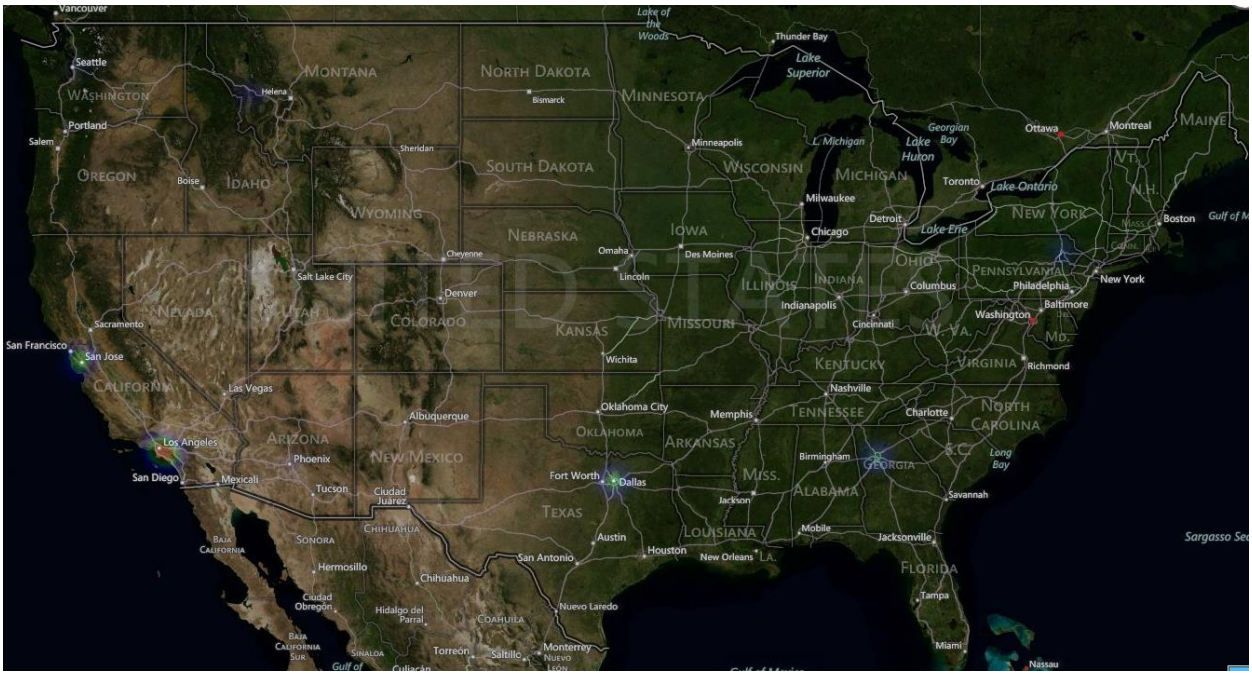


Figure 7: The U.S. has the second largest number of Nitol-controlling servers. U.S.-based computers that control the Nitol family of malware primarily appear in California, Texas, Georgia, and Pennsylvania. Servers in San Diego, San Jose, Dallas, Atlanta, and Scranton, control the vast majority of the infection's daily operations in America.

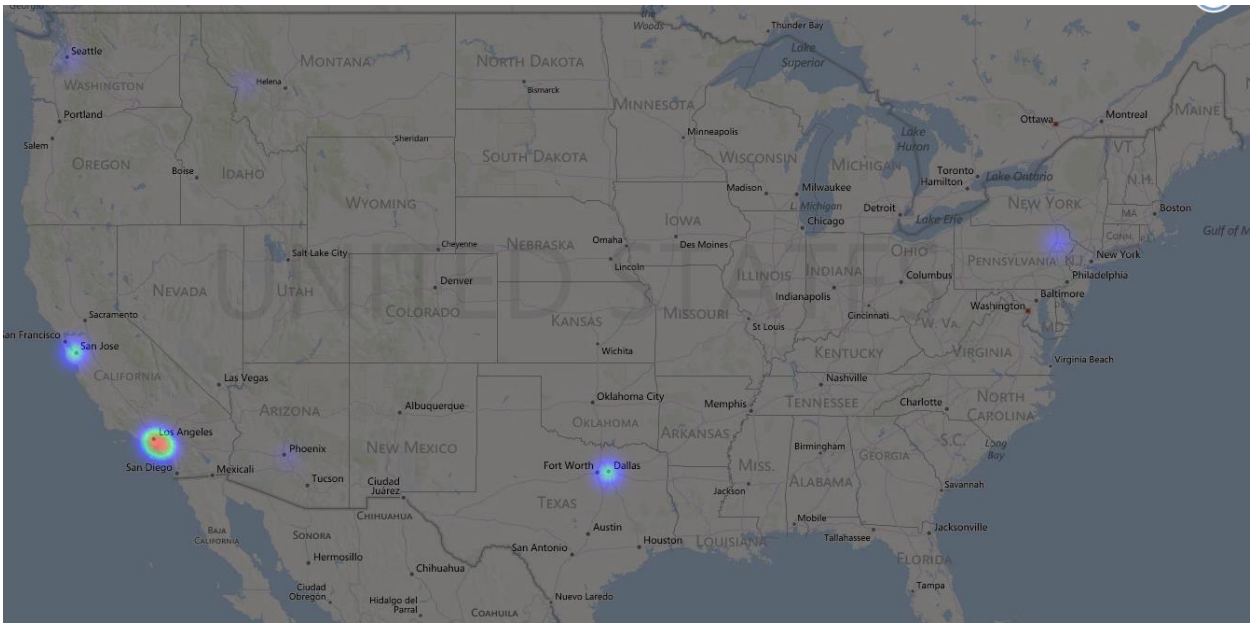
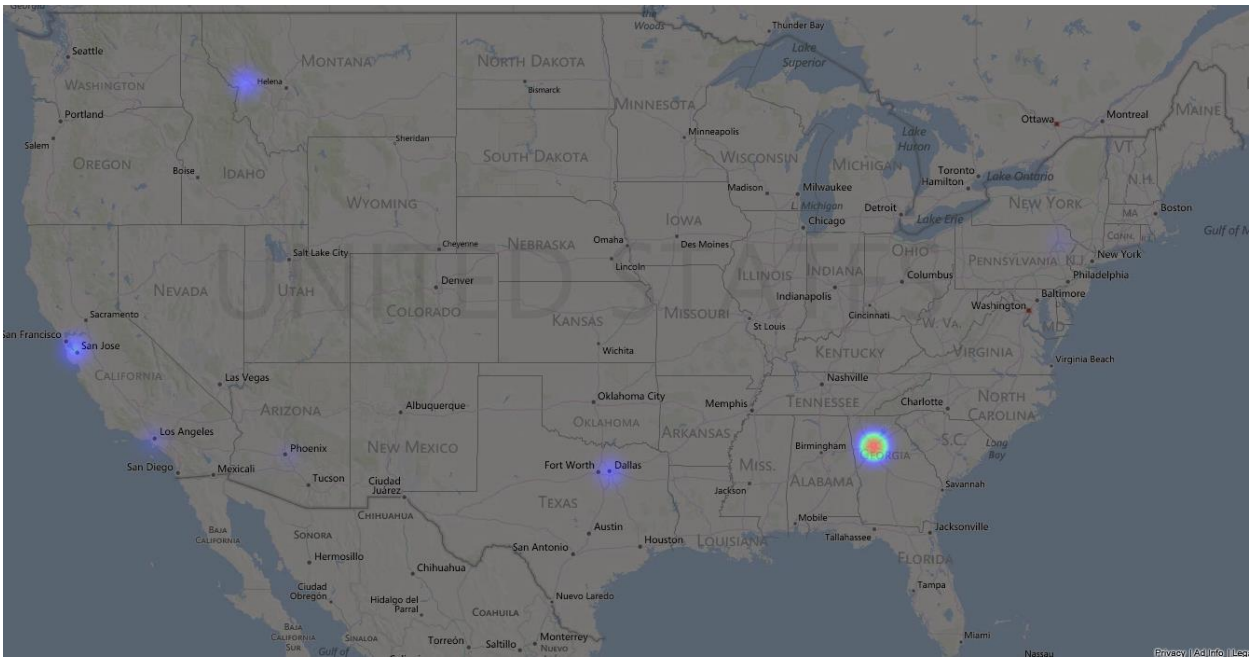


Figure 8: Nitol.A (above) C&C locations compared with Nitol.B (below) C&C locations.



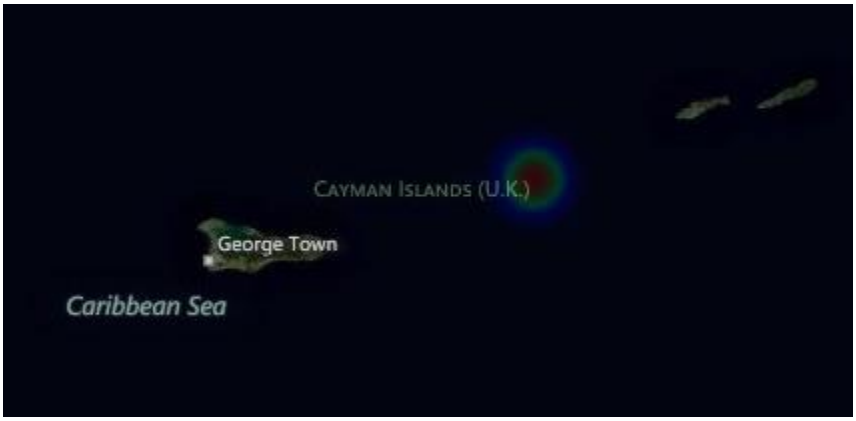


Figure 9: Following China and the U.S., the Cayman Islands has the third-highest number of Nitol-controlling servers.

DCU analyzed all Nitol variants collected by MMPC. This analysis shows that a vast majority of collected samples connect to subdomains of 3322.org to retrieve the IP address of their primary C&C servers. The below graph demonstrates the extent to which this domain is used by the virus.

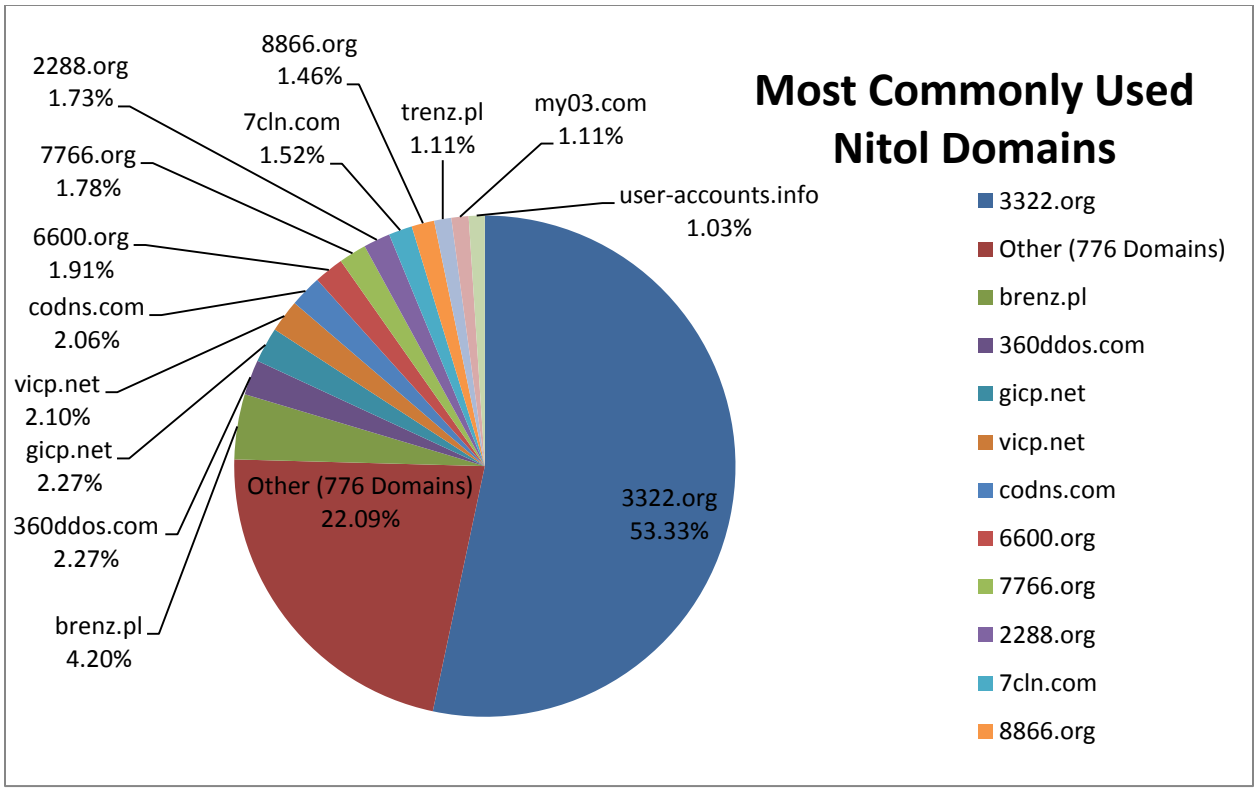


Figure 10: Over half (55%) of the Nitol samples obtained by MMPC use 3322.org for their C&C domains.

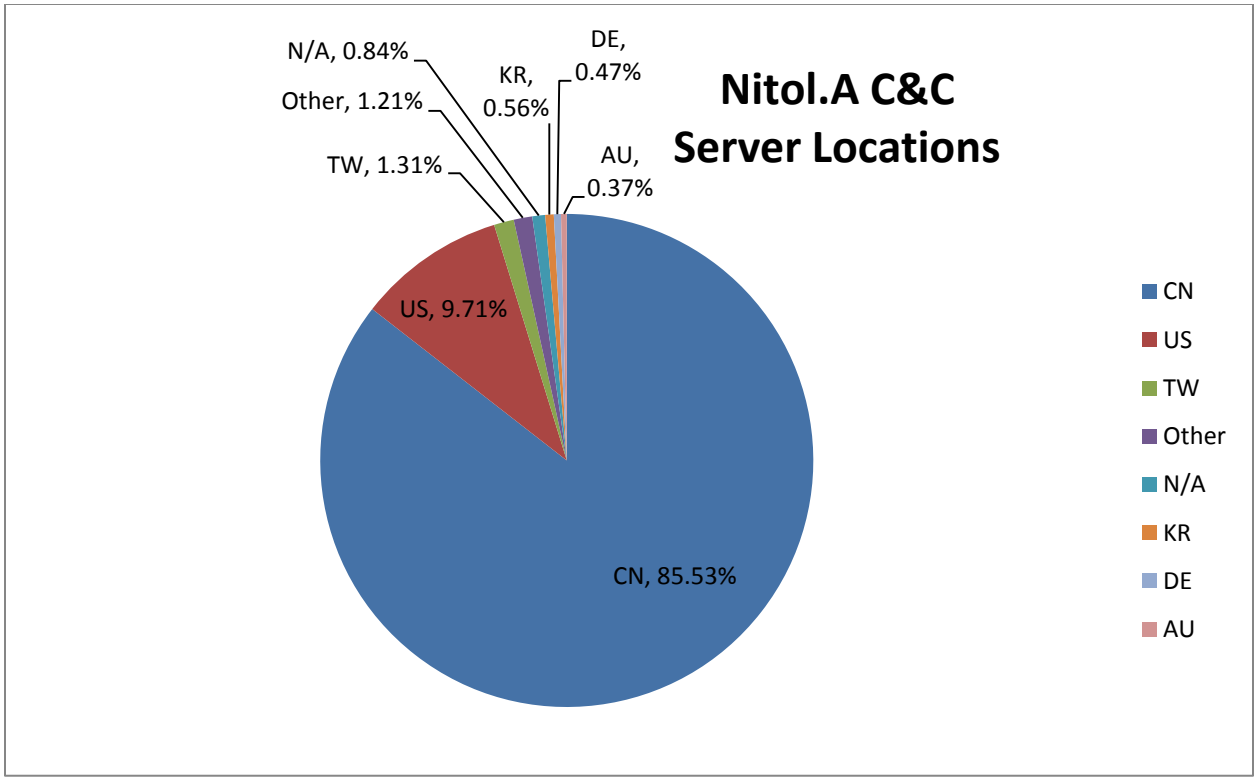


Figure 11: The vast majority of Nitol.A infections connect to servers located in China.

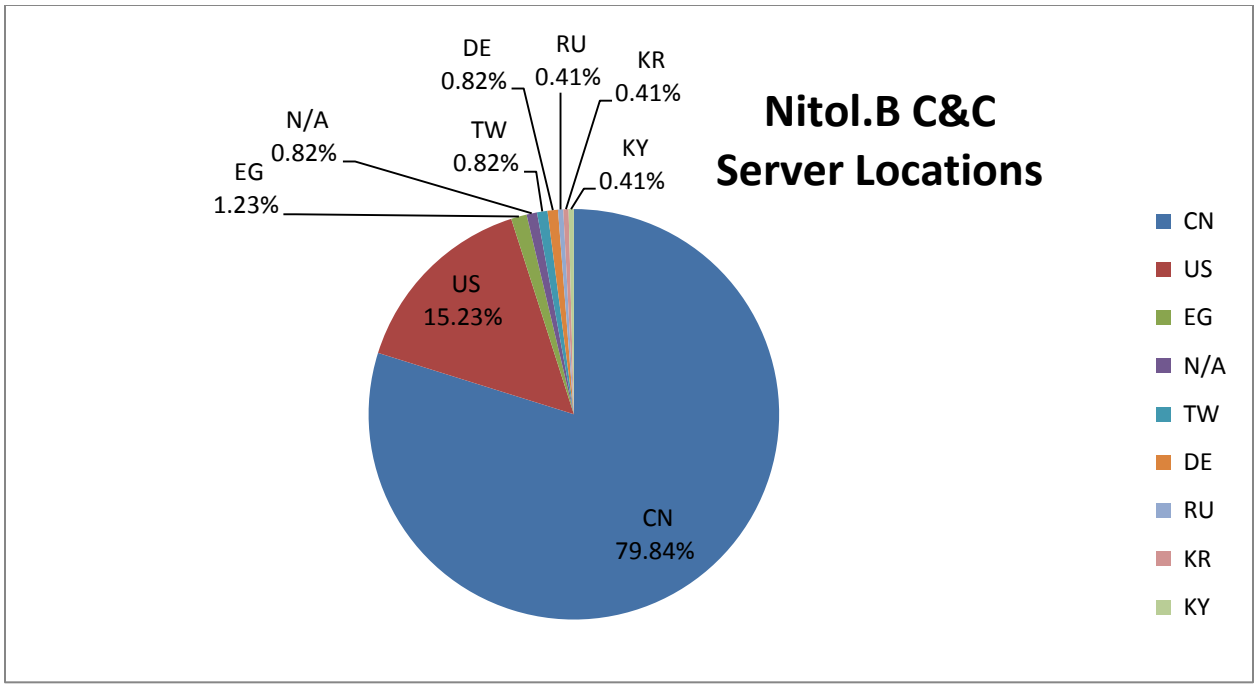


Figure 12: Similar to Nitol.A, the .B variant receives instructions from servers located in China.

Figure 13: Malware connecting to 3322.org retrieves IPs to C&C servers in the following regions in the U.S., Canada, Mexico, and Central America.

Figure 14: Malware connecting to 3322.org retrieves IPs to C&C servers in the following regions in China.

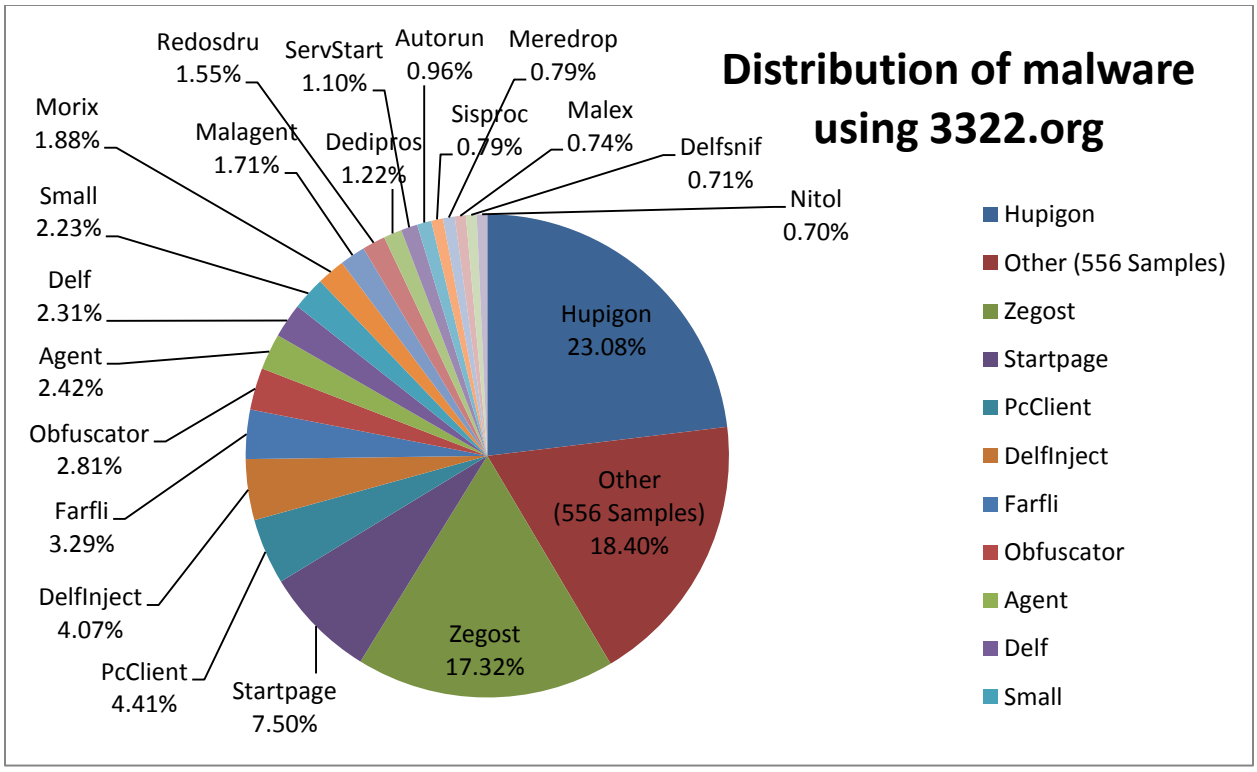


Figure 15: The above graph represents the distribution of malware currently utilizing 3322.org to retrieve C&C server IP addresses.

Malware Name	Purpose
Hupigon	Allows a remote attacker to control a victim's web camera, microphone, take screen shots, and copy or delete user files on the infected computer.
Zegost	Connects to a C&C to receive instructions capable of executing any behavior the attacker wants.
StartPage	Changes a victim's Internet Browser home page without consent.
PcClient	Enables keylogging, creates a backdoor, and operates as a rootkit. Part of the Trojan family of malware.
DelfInject	Copies and installs software on victim's computer. Commonly installs a remote backdoor which allows an attacker surreptitious access to infected systems.
Farfli	Typically directs victims to web sites not of their choosing. Also has backdoor capabilities that allow it to connect to a remote attacker and wait for instructions.
EggDrop	Sets up attacks by disabling the Fast User Switching feature in Windows to allow multiple remote desktops to connect to an infected box. So far, the malware appears to be an attack that trampolines on Window's built-in remote desktop functionality to give user full access to victim system.
Nitol	Performs DDOS attacks, spreads through removable and network devices, and allows attacker to run software of their choosing on the victim's computer.

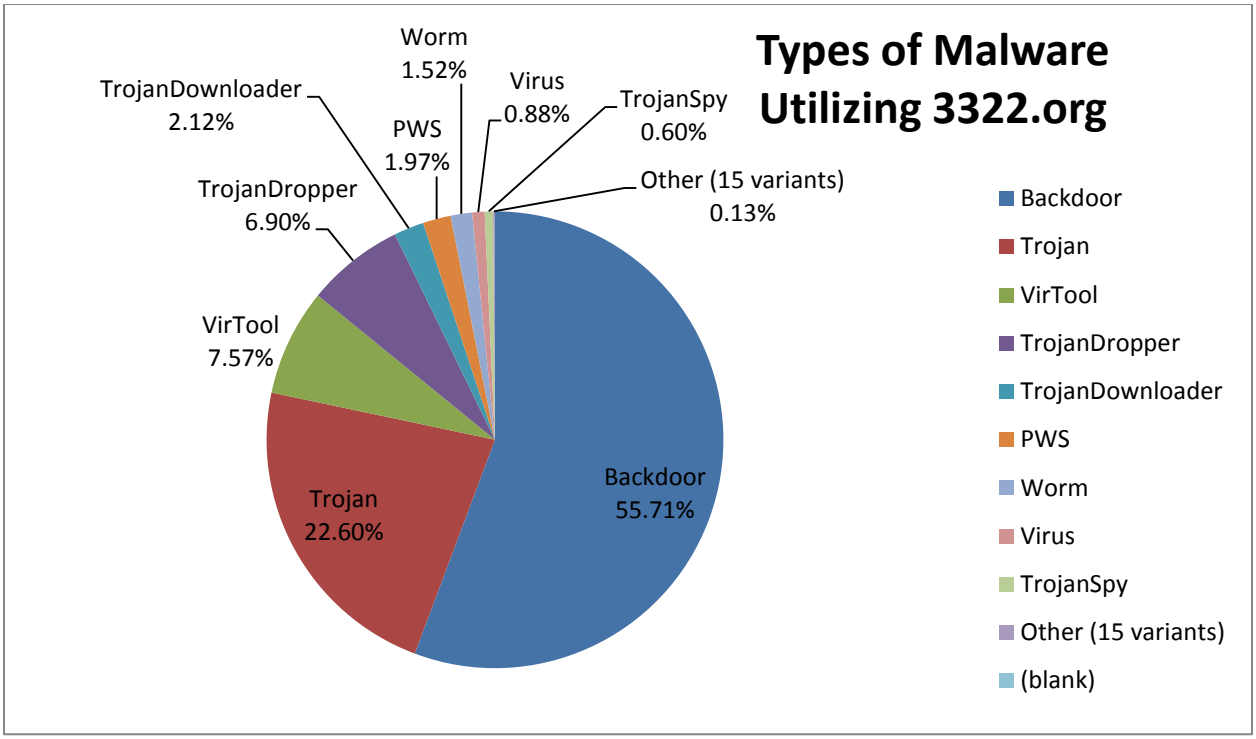


Figure 16: Distribution of the types of malware developed to utilize 3322.org as a C&C intermediary.

Malware Type	Purpose
Backdoor	A backdoor allows an attacker to perform the same activity as the user that is compromised, including turning on the computer's built-in microphone or video camera to listen in or watch people's conversations. It also allows an attacker to take screenshots, copy/move/delete files, and perform keylogging to steal a victim's personal information.
Trojan	Typically packaged to look like legitimate software, a Trojan contains source code that can compromise a victim's computer to install any of the other types of additional malware onto an infected computer.
Virus Tool	A Virus Tool is a generic classification given to applications that are primarily used to create, obfuscate, or facilitate the making or distribution of malware.
Trojan Dropper	A Trojan Dropper is an application whose sole purpose is to download and execute software on a victim's computer. It is also used to denote an application that is downloaded and executed on a victim's computer.
Trojan Downloader	A Trojan Downloader is application whose sole purpose is to download files onto a victim's computer. It is also used to denote an application that is copied onto a victim's computer.
PWS	A PWS is a Password Stealer. This type of malware logs user keystrokes or retrieves text typed by the user with the sole purpose of obtaining user credentials.
Remote Access	A Remote Access is an application that allows remote connections to a victim's computer. This program, once run on a computer, allows a cybercriminal to control a computer's visual/keyboard/mouse/audio

	features.
Browser Modifier	A Browser Modifier typically a website or denotes an application that replaces search results, URL navigation, WPAD or DNS resolution, and/or click information with destinations of the attacker's choosing.