1.1 OVERVIEW / The Prolexic Security Engineering and Response Team (PLXsert) recently analyzed the Asian distributed denial of service (DDoS) crimeware kit known as Storm Network Stress Tester. This crimeware kit should not be confused with the Storm botnet that infected millions of computers in 2007. The Storm crimeware kit can generate up to 12 Mbps of attack traffic leveraging a single infected host with a single attack vector. However, Storm is designed to support up to four simultaneous DDoS attack types and can generate significant payloads when used in attacks involving a large number of compromised hosts. In addition to its multiple DDoS attack capabilities, it can be used to manipulate infected hosts remotely.

1.2 INDICATORS / Storm has a client-server architecture: an infected host will connect to a command-and-control (CC or C2) server. It infects Microsoft Windows machines (XP and later). Once installed on a victim Windows machine, Storm exposes Remote Administration (RAT) capabilities, enabling malicious actors to execute commands on the infected host.

Storm Network Stress Tester has the capability to execute multiple DDoS attack types on infected hosts, including UDP, TCP and ICMP. Details of the architecture, forensic traits, infection process and DDoS payloads of the tool are provided in this threat advisory.

Figure 1: The command and control (CC or C2) application
1.3 ARCHITECTURE / The Storm Network Stress Tester user interface is used to build payloads and acts as the command-and-control server (C2). In addition, it provides the malicious actor with several remote (RAT) functions, including directory traversal, file uploading and downloading, execution, and DDoS attack capabilities.

Once the Storm Network Stress Tester C2 is running, it opens a listening socket on the attacker’s PC on port 1990, as shown on the Process Hackers Network tab in Figure 2. This port will wait for incoming connections from infected zombie PCs.

1.4 PAYLOAD GENERATION / The payload creation option generates the executable that will be used to infect zombies. These zombies will then serve as clients to the C2. The strings for the IP address and port are hardcoded into the payload, and are used to connect back to the C2, authenticate, and wait for commands.
1.5 BINARY PAYLOAD INFECTIONS / The dropper payload that is generated by the C2 is named DDoS.exe by default. (Note: DDoS.exe is not a major indicator; it can be renamed to anything an attacker wants.) The dropper payload, which includes the IP address and port as specified in the user interface, is used to infect any number of hosts to be used in a botnet.

The binary has some identifiable strings, as shown in Figure 4, which can help categorize its potential behavior.

Windows China Driver is the name that the service displays once the payload runs. It also persists on the zombie PCs, as shown in Figure 5.

When the DDoS.exe binary is run, it dumps two payloads onto the victim’s system directory: ntserver.exe and ntserver.dll. Before the payloads are executed, DDoS.exe will prepare the persistence for the ntserver.exe service utilizing registry changes. It adds the registry key, “Made in China DDoS,” to “HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\.” Once the registry key is added, the service executable is run using the CreateService() API.

During the execution of this crimeware on a Windows 7 operating system in the PLXsert lab, it was necessary to disable user access control (UAC) in order to execute the payload. In a real world situation, the attacker would need to find more creative and covert methods to bypass this security feature.
Such action is typically accomplished by taking advantage of vulnerabilities in a browser or desktop application, which would allow the payload to be downloaded and executed (with the appropriate permissions) on the unsuspecting victim’s PC. There are indications that the infection rates for this tool are likely to be higher on pre-Windows Vista operating systems, which lack the user access control mechanism.

1.5a THE CHINESE CONNECTION / China has a reputation for having high rates of pirated software and Windows XP is the most prevalent operating system in the country, accounting for about 60 percent of desktop operating systems.

With that demographic and all the Chinese references, it appears this tool had been designed to exploit victims running Windows XP operating systems in Asia.

1.6 FORTIFICATION / The payloads dropped by DDoS.exe, ntserver.exe and ntserver.dll, are critical components for infecting zombie PCs. Ntserver.exe persists as a service and will ensure that the connection to the C2 is active when a PC restart is performed. Ntserver.dll is the injected library found in an infected Internet Explorer process created by the ntserver service.

1.6a NTSERVER.EXE / Ntserver.exe is the service executable that is started by DDoS.exe and persists as a Windows service. Its purpose is to start the iexplorer.exe process with elevated privileges (Session 0) without spawning a user interface and then injecting the ntserver.dll. This will provide both stealth and proper access elevation for communication between the zombie and the C2.

Figure 6: The injected iexplorer process running as SYSTEM
Once the dll is injected, it will establish a connection with the C2 at the IP address and port specified when it was generated. Once ntserver.exe has executed the hidden Internet Explorer process with the injected dll, its job is complete and it merely provides persistence on the infected PC.

1.6b TSERVER.DLL / The ntserver dll is the most important piece of the infection. It is through this library (see Figure 7) that the attacker will communicate and control the zombie PC. In order to establish the connection to the C2, the zombie, upon infection, will send a payload that consists of a hard-coded integer password (123456) and information about the infected PC. The structure of this initial payload is shown in Figure 8.

Figure 7: The ntserver.dll module present inside of iexplorer.exe

```c
typedef struct SYSINFO
{
    DWORD yzm; //123456 auth passcode
    int ver;
    DWORD cpu;
    DWORD mem;
    char curname[100];
}SetSYSINFO;
```

Figure 8: The structure of the initial payload

Figure 9 provides an example payload of this authentication, as sent from the infected zombie to the C2 server. Notice the bolded hex value 40e20100 (0x00001e240) is 123456 in decimal, which the C2 uses to determine whether to accept the incoming connection or not.

Figure 9: The payload authentication sent from the zombie to the C2 server
Once the connection has been established, the client waits for commands from the C2. These commands can range from launching DDoS attacks to remote disk operations and file execution. The command structure is dissected in the next section.

1.7 COMMAND STRUCTURE / Understanding a C2’s command structure is vital to identifying, communicating with and possibly taking down the C2 itself. We’ll review its components one by one. The first command structure is shown in Figure 10.

```
typedef struct DDoS
{
    DWORD msg_id;
    char addr[255];
    int port;
    int time;
    int xci;
    int pt;
    char wParam[256]; //document management info
    int lParam;//file transfer info
}GETDDOS;
```

Figure 10: Command structure A

msg_id can be defined as any one of the commands shown in Figure 11.

```
#define CDDOS 0x01
#define C_STOP 0x02
#define C_REMOVE 0x03
#define C_GETDRIVE 0x04
#define C_SHOWFILELIST 0x05
#define C_UPLOADFILE 0x06
#define C_DOWNLOADFILE 0x07
#define C_FILEDEL 0x08
#define C_REMOTERUN 0x09
#define C_SYSTEMINFO 0x15
```

Figure 11: Command structure B used to define Storm Network Stress Tester capabilities

The pt field is an integer check that specifies the DDoS attack to execute. These are the commands responsible for launching DDoS attacks (Figure 12).

```
1 = UDP
2 = SYN
3 = TCP
4 = ICMP
5 = CC
6 = MONI
7 = SJLW (unimplemented)
```

Figure 12: Command structure C defines attack vectors
Other components include:

- xc is used for the stop command, terminating all associated threads
- m is the parameter for remote run and delete file commands
- wParam holds a string of 256 characters max (including null terminator)
- lParam is used for download and upload file functions and takes the port number

The msg_id and pt fields define the types of DDoS attacks that the zombie PCs carry out, as commanded by the C2. A msg_id value of 1 instructs the zombie to perform a denial of service attack. The zombie then checks the pt value to parse which type of attack to execute.

1.8 LAB SETUP AND ATTACK SIGNATURES / PLXsert set up a lab environment to gauge the capabilities of the tool, to simulate the attack flow of the attack and capture attack signatures. Figure 13 diagrams the attack flow lifecycle as it might occur during a real infection and attack.
The malicious actor uses the Storm Network Stress Tester UI to send attack commands to the zombies, which will then execute the attack. Attacks in the lab tests were performed with predefined settings and recorded using tcpdump. The results of these recordings are discussed below.

1.8a UDP ATTACK / Figure 14 shows the payload of a UDP attack. The payload consists of a repetition of the character A or hex value 0x41 with a length of 1024 bytes.

1.8b TCP FLOOD / The TCP flood sends a data segment of predefined characters, as shown in Figure 15. These are split according to the maximum segment size (MSS) value on the receiving end. In the example shown in Figure 15, we see two 1460-byte packets followed by a 1024-byte packet with the Push flag set.

The C2 and IE cache flood each send HTTP GET requests to the specified target. The signature of the GET request is shown in Figure 16.
1.8c ICMP FLOOD / The ICMP flood (Figure 17) uses the same buffer payload as the TCP flood. Packets are fragmented according to the MTU size on the receiving network.

![Figure 17: The payload of the Storm Network Stress Tester ICMP flood](image)

1.8d SYN FLOOD / Several attempts were made to test the SYN flood feature of the Storm Network Stress Tester crimeware kit. However it was determined that this feature was either not implemented correctly or not implemented at all, as a result there were no payloads recorded for this attack type.

1.9 CONCLUSION / The analysis of the Storm Network Stress Tester crimeware kit illustrates how readily malicious actors have been able to set up and control a botnet. When coupled with a high infection rate, attackers have been able to launch major DDoS attacks against their targets.

Security features in newer Windows operating systems can make this crimeware kit less effective, but more sophisticated attackers have bypassed these limitations and increased the rate of infection. Storm Network Stress Tester still poses a threat to the many Windows XP machines that are ran still in use throughout the world, including those in China. PLXsert plans to continue to monitor this crimeware kit and identify any future related DDoS threats.
The Prolexic Security Engineering and Research Team (PLXsert) monitors malicious cyber threats globally and analyzes these attacks using proprietary techniques and equipment. Through research, digital forensics and post-event analysis, PLXsert is able to build a global view of security threats, vulnerabilities and trends, which is shared with customers and the security community. By identifying the sources and associated attributes of individual attacks, along with best practices to identify and mitigate security threats and vulnerabilities, PLXsert helps organizations make more informed, proactive decisions.

Akamai is a leading provider of cloud services for delivering, optimizing and securing online content and business applications. At the core of the company’s solutions is the Akamai Intelligent Platform™ providing extensive reach, coupled with unmatched reliability, security, visibility and expertise. Akamai removes the complexities of connecting the increasingly mobile world, supporting 24/7 consumer demand, and enabling enterprises to securely leverage the cloud. To learn more about how Akamai is accelerating the pace of innovation in a hyperconnected world, please visit www.akamai.com or blogs.akamai.com, and follow @Akamai on Twitter.

Akamai is headquartered in Cambridge, Massachusetts in the United States with operations in more than 40 offices around the world. Our services and renowned customer care enable businesses to provide an unparalleled Internet experience for their customers worldwide. Addresses, phone numbers and contact information for all locations are listed on www.akamai.com/locations

©2014 Akamai Technologies, Inc. All Rights Reserved. Reproduction in whole or in part in any form or medium without express written permission is prohibited. Akamai and the Akamai wave logo are registered trademarks. Other trademarks contained herein are the property of their respective owners. Akamai believes that the information in this publication is accurate as of its publication date; such information is subject to change without notice. Published 04/14.