Connecting and Protecting
the Networked World℠

Collaborative Steps to Breaking Botnets:

How Level 3 and Cisco Worked Together to Improve the Internet's Security and Stop SSHPsychos

Level 3℠ Threat Research Labs

April 16, 2016

Collaborative Steps to Breaking Botnets: How Level 3 and Cisco Worked Together to Improve the Internet's Security and Stop SSHPsychos

The information security community's ability to respond to threats and vulnerability discovery improves with each passing month. The collective reaction from the security community to a new file hash, new technique, or communication method has never been stronger. However, attackers are also keeping up, or even exceeding the security world's defenses.

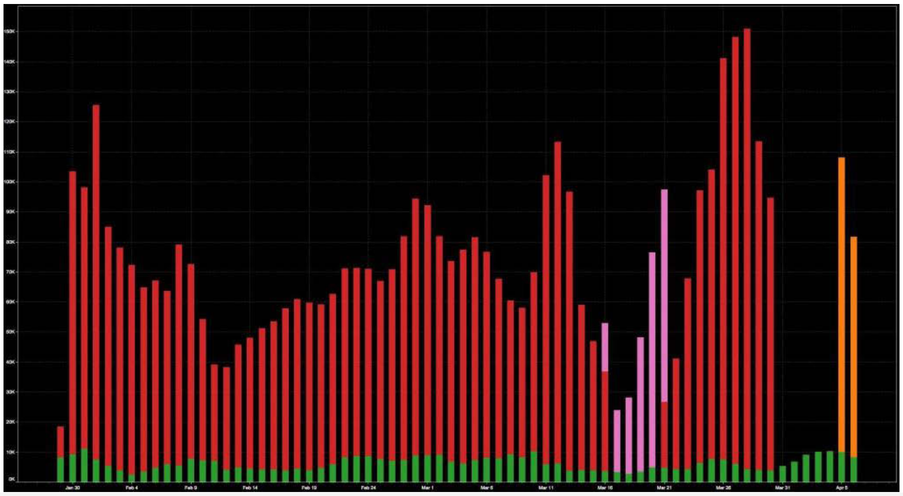
One way to balance this problem is to not only focus on identifying the threat, but also to find an effective method of removing it from the Internet. Too often problem identification is confused with problem removal, leaving attackers observed, yet still able to pursue their goals.

This is why Level 3's Threat Research Labs and Cisco's Talos Group worked together to investigate and mitigate the risk posed by an attacker's Internet-wide scanning and DDoS botnet, SSHPsychos.

Investigating Malicious Actors

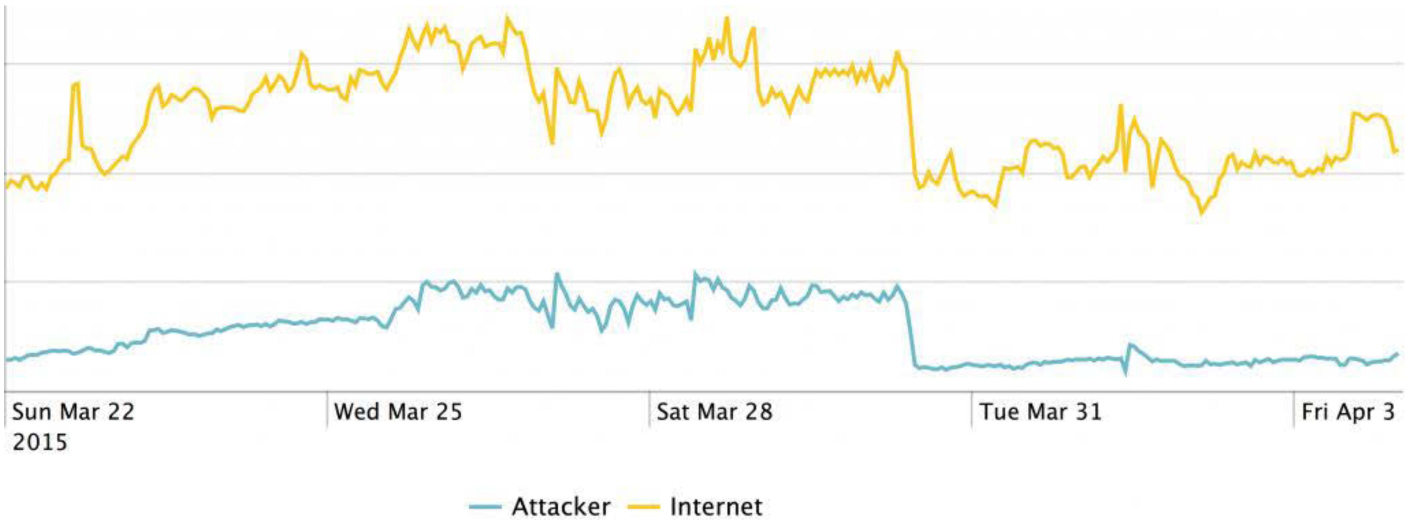
In late September 2014, the *Malware Must Die!* Blog detailed a new Linux malware and rootkit used for DDoS attacks. Despite their well-documented description, the threat persisted. More than four months later, FireEye identified an unusually large SSH brute force attack attempting to load the same malware, which was functioning as an extremely effective rootkit and DDoS tool when coupled with SSH brute force login attempts.

Fortunately for the Internet community, the Talos Group at Cisco did not stop tracking the campaign. In Q1-2015, Talos' honeypots saw more authentication attempts from this single attacker (103.41.125.0/23 and 43.255.190.0/23) than all other hosts combined.



Source: Cisco Talos Group. RED/PINK/ORANGE – Attacker. GREEN – Rest of Internet

In late March, Level 3 began discussions with the Cisco Talos Group to work together to mitigate this threat to the Internet. Level 3's network data confirmed the massive scale that this attacker attained when compared with overall Internet traffic for SSH. At times, this single attacker accounted for more than 35% of total Internet SSH traffic.



Source: Level 3 Research Labs BLUE- Attacker, YELLOW- Rest of Internet

Clearly the security community's awareness of the overall event was not enough to discourage the attacker. An action more substantive would have to be taken for any improvement to occur.

The team's goal, when an Internet risk is confirmed, is to remove it as broadly as possible; however, before blocking anything from the Internet, it is important to fully understand the impact that it may have to more benign hosts. To do this, the research group will examine the attacker's tools and infrastructure in greater detail.

In this case, The Talos Group's honeypot data allowed the Level 3 team to identify what actions were taken after a successful brute force root SSH login occurred. The chain of events led to the download of a file from a web server running on 23.234.60.140 (resolved from ftp.rxxiaoao.com) and 23.234.19.202. The first host serves files within /install named 8000.rar through 8008.rar, and the second host a06 through a11 within the /i directory.

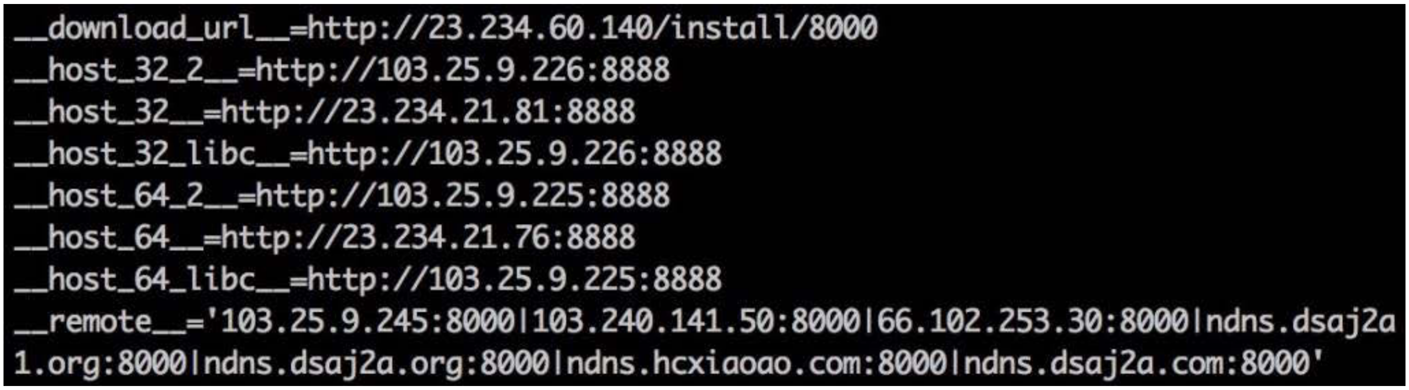
Upon downloading the files, the Level 3 Threat Research team confirmed the information supplied in the *Malware Must Die!* blog from September, the filename is structured to be aligned with the port on which the eventual botnet communication will occur. However, the attacker had moved on from port 3502 through 3505 that were used back in September and was now making use of TCP ports 8000 through 8008 and 3306.

The first host’s file is a more detailed shell script, which provides an insight to some of the logic used by the attacker. Although named with a .rar extension, each file is actually a Unix shell script, using the same obfuscation as from September:

```
dec(){ echo $@|tr “[a-zA-Z0-9\;-=+*\/]” “[.0-9a-zA-Z\/\/\:]”; }
```

The translation string had not changed at all.

This simple bash function dec() takes obfuscated text and translates characters back to the intended text. With this function one can extract the interesting strings from the 8000.rar file retrieved:



```
__download_url__=http://23.234.60.140/install/8000
__host_32_2__=http://103.25.9.226:8888
__host_32__=http://23.234.21.81:8888
__host_32_libc__=http://103.25.9.226:8888
__host_64_2__=http://103.25.9.225:8888
__host_64__=http://23.234.21.76:8888
__host_64_libc__=http://103.25.9.225:8888
__remote__='103.25.9.245:8000|103.240.141.50:8000|66.102.253.30:8000|ndns.dsaj2a
1.org:8000|ndns.dsaj2a.org:8000|ndns.hcxiaoao.com:8000|ndns.dsaj2a.com:8000'
```

Source: Level 3 Research Labs

The most important lines here are the __download_url__ variable where the actual executable is retrieved and the __remote__ variable, which is used for command and control communication.

The only difference between each script (8000.rar vs 8008.rar for example) is the __download_url__ filename and port numbers for __remote__ change, which match the number from the filename of the script.

After confirming that nothing structural had changed in the malware, the Level 3 Threat Research Labs loaded it inside a CentOS 7 VM as root and watched it work.

Monitoring Botnet Communication in Action

After retrieving and executing the binary executable from the __download_url__ at 23.234.60.140 and 23.234.19.202, the bot immediately begins searching for its command and control host. The executable has hardcoded 8.8.8.8 and 8.8.4.4 as its DNS resolvers and proceeds to attempt DNS resolution for the hostnames configured. Next, it attempts connections to the IPs and resolved hostnames that were contained within the __remote__ line of the shell script.

In the case of the research team's VM, the various versions of the malware were able to establish connectivity to C2s at the following IP addresses:

- 103.240.140.152 (resolved from ndns.dsaj2a.org and ns2.hostasa.org)
- 162.218.112.7 (resolved from ndns.dsaj2a1.org)
- 104.143.5.25 (resolved from ndns.dsaj2a1.org and ns1.hostasa.org)
- 103.240.141.54 (resolved from ndns.dsaj2a.com, ndns.hcxiaoao.com, and ns3.hostasa.org)

Other communication behaviors were as expected: As part of a DDoS botnet, the research team's bot was instructed to launch SYN floods each time it connected to the C2. The SYN packets were null padded to maximize bandwidth usage and did not bother to spoof their origin. The communication from the C2 instructing the team's bot to attack was confirmed to be XORed with the same key (BB2FA36AAA9541F0) that had been in use since the original malware research.

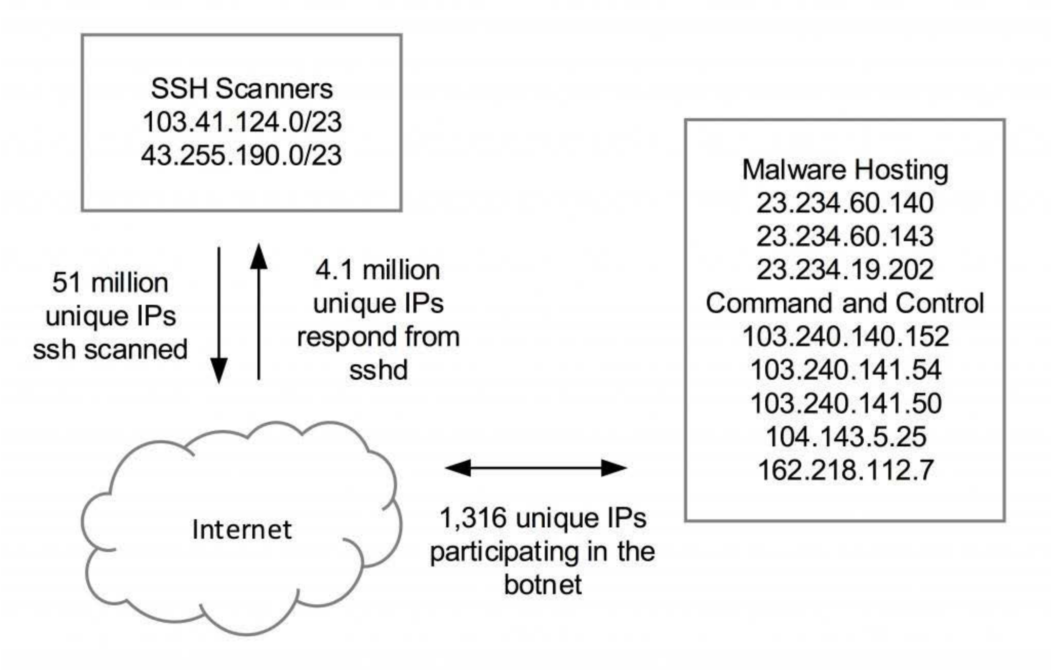
The other noteworthy communication was the every 30 minute retrieval of /config.rar from the original malware hosted site (23.234.60.140), this time by resolving the hostname info.3000uc.com. The file was retrieved with the user-agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; TencentTraveler ; .NET CLR 1.1.4322)

This file, as with the others, was not a RAR file, but this time was XORed with the same 128bit key as the C2 communication. After decoding it, the team found a configuration file containing the following keys: md5, denyip, filename, and rmfile. These contain values referencing a number of other known trojans and malware. Researchers at avast! confirmed that the config is used to remove and kill competing malware so the bot can have full control of the machine. The current contents of the decoded file can be read here as a helpful source to find indicators of compromise from other attackers.

Having confirmed what the malware does, how it communicates, and with whom it is speaking, the researchers began to assess its impact to victims on the wider Internet.

Victim Impact

Over a two-week period in late March and early April, the Level 3 Research Labs monitored a large number of IPs scanned by the attackers. They also identified which hosts in the Internet were active participants in the botnet. Of the botnet hosts, the team identified that C2 communication was occurring over TCP ports 8000-8008 and 3306, as seen in the current version of the malware. However, a number of hosts were still communicating over TCP ports 3502-3508 as seen in previous versions.



The team, after assessing the massive scale, impact, and duration of this threat, determined that it was necessary to work on a strategy to take this malicious infrastructure off the Internet. The Cisco Talos team concurred with this assessment.

Takedown

On Tuesday, April 7, 2015, Level 3 took action by blackholing all attacker traffic inside of its global networks. This ensured that no traffic to the attacker would be successfully sent through Level 3. The Level 3 Security Operations team began outreach to other network operators, briefing them on the threat, and requesting that they also follow suit in removing it from the global Internet permanently.

Level 3 Research Labs continues monitoring the attacker’s actions to maintain awareness of any changes made to the attack infrastructure. Throughout the analysis period the attacker shifted their SSH scanning operation from 103.41.124.0/23 to 43.255.190.0/23, along with shifting multiple C2 and malware IPs. The team’s recommendation is for all organizations to maintain awareness of SSH scanning in this address space, and as with most threats the expectation is that this attacker will attempt to resurrect their DDoS capability.