Level 3 COMMUNICATIONS

Connecting and Protecting the Networked World℠

SAFEGUARDING **THE INTERNET**

LEVEL 3 BOTNET RESEARCH REPORT

JUNE 2015

SAFEGUARDING THE INTERNET | LEVEL 3 BOTNET RESEARCH REPORT

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

Today, none of us are immune to the impact of botnets on Internet-connected organizations. There is ample validation that monitoring the communications patterns between command-and-control servers and their intended victims is vital. We believe that taking a proactive approach to tracking botnet behavior can yield threat intelligence that is truly actionable. Botnets that are used for DDoS attacks are on the rise, but so are other types. This report examines the potential causes for the increase in these attack types, the profile of the victims by industry and geography, commonly-targeted ports and protocols, and several other botnet characteristics.

We take a closer look at botnets that are used specifically to deploy malware (such as the recently uncovered SSHPsychos and PoSeidon) to gain insights into complex threat models and protection options. These use cases serve to raise awareness of what organizations should expect from their network service providers, and highlight the need for greater levels of partnership and collaboration across the security community to safeguard the Internet more effectively.

We hope you find this research a valuable resource in your efforts to protect your organization, and the connected world.

Chris Richter
Senior Vice President of Managed Security Services
Level 3 Communications

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

Executive Summary

Threat intelligence is only useful if you can take action quickly to protect networks, systems and data. Organizations today are challenged with a high volume of security events produced by the ecosystem of their non-collaborative security solutions. It is not a question of receiving intel on attacks, but rather: What data should you use to find indicators of critical security threats?

As a global network services provider, Level 3 has an expansive view of worldwide Internet traffic and a broad view of risks. Our 24/7 Security Operations team, a group of trained security professionals, monitors approximately 45 billion NetFlow sessions per day to protect our network. With a broad lens of two-way communications across the Internet, the team sees victim computers around the globe connecting with bad actors. Every day, our security team monitors approximately 1.3 billion security events and mitigates roughly 22 distributed denial of service (DDoS) attacks. The team identifies, and removes, on average, one control and command server (C2) network per day. The goal is to share insights about the global threat landscape from the Level 3 perspective, and to offer best practices for effectively protecting information assets.

In our research, we pay specific attention to trends in botnet behavior, DDoS attacks and malware. Malicious actors use these tools to gain control of corporate assets and turn them into compromised endpoints. They use these infected machines to distribute malware, disrupt business, establish system penetration and steal company intellectual property (exfiltration). Out of the more than 1,000 C2s we tracked during the first quarter of 2015, we found over 600 being used for malicious communications targeting corporate environments. Left unchecked, these C2s have the potential to disrupt business and destroy critical information assets.

We derive threat data by sampling communication flows across our network each day. We correlate this data with Level 3's reputation database, which produces risk rankings based on a proprietary, threat-scoring schema. This threat-scoring schema is derived from the Level 3℠ Managed Security Services systems, algorithmic research on NetFlow and third-party reputational data feeds.

This Internet-wide threat communications data complements other information sources, such as honeypots, which help security professionals protect their data, systems, and networks worldwide.

With this threat data, we take actions on our backbone, our customers' networks and the Internet, if necessary, to mitigate and prevent a range of attack types. In this report, we will discuss our findings and actions based on our work with this intelligence and analysis.

SAFEGUARDING THE INTERNET | LEVEL 3 BOTNET RESEARCH REPORT

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

TABLE OF CONTENTS

A BASELINE ON BOTNETS

Botnets are a group of Internet connected programs resident on various devices communicating together to perform tasks. These devices can be Web servers, personal or work computers, mobile devices or cable modems.

Botnet tasks include scanning new targets, exfiltrating data, distributing malicious software (malware such as viruses, worms and keyloggers), stealing personal information or intellectual property, or attacking other targets (e.g. DDoS attacks).

Most of the machines that are a part of the botnet are also victim machines. They are infected through a number of methods, including phishing emails, visiting compromised sites or installing compromised software.

Command and control servers (C2s) are the brains of the operations. C2s issue instructions to infected machines to perform a task like an attack.
Common formations for botnets are:

Single Server: One C2 manages all of the infected machines. This simple configuration provides reliable, low-latency communication. Once discovered, it's easy to take down.

Multiple Server: Several C2s are meshed for redundancy.

Hierarchical: Multiple C2s in a partitioned configuration enable multiple tasks and help obfuscate the botnet's scale from researchers.

Peer to Peer: Bot-to-bot communications are more challenging to track and take down.

Stranger Danger: The importance of monitoring two-way communications with command and control botnets.

C2 communications are a direct indication of risk potential or compromise. Among the methods used to generate our threat intelligence is monitoring and analyzing two-way communication patterns of C2s. With customers in more than 60 countries spanning six continents, Level 3 has an exceptional view of the networked world and the malicious actors that attempt to compromise the flow of critical business information. From our global Internet vantage point, the team has visibility into the span of control of these malicious actors and the number of victims impacted — or potential risks. We see the reach and damage of threat sources, and at the same time, determine the impacts to individual servers or hosts. In the first quarter, significant C2 communications originating from points in countries including Ukraine, Russia and the Netherlands targeted potential victims in the United States. Our analysis techniques allow us to see the movement of these actors and take action against those that posed a threat to our network. Botnets do not stand still. In the SSHPsychos use case, we discuss how we use communications data to track these sophisticated threats across the Internet.

FOR THE PURPOSES OF THIS REPORT, A "VICTIM" IS DEFINED AS ANY ENDPOINT COMMUNICATING WITH THE C2. THE VICTIM MAY BE TARGETED WITH THE INTENT OF EXTRACTING DATA FROM IT. THE VICTIM ALSO MAY BE USED AS A BOTNET, AIDING IN ACTIVITIES OF THE C2 TO TARGET OTHER VICTIMS. MANY BOTNETS ARE HOSTED BY LEGITIMATE COMPANIES IN LEGITIMATE INFRASTRUCTURE. LEGITIMATE HIGH-TRAFFICKED DOMAINS ARE OBVIOUSLY USEFUL DISTRIBUTION MECHANISMS FOR MALWARE AND PHISHING.

Trend Alert: Movement to Cloud

Not unlike commercial enterprises and other legitimate organizations, cybercriminals are realizing the benefits of spinning up instances on virtual machines. Cloud providers, in some cases, require limited data validation to set up an account. A simple PayPal® account or a stolen (but still valid) credit card, can be used as a means of paying for these services. Establishing rogue virtual machines (VMs) on Infrastructure as a Service (IaaS) cloud service providers is thus an attractive model for these "customers." Therefore, it is our belief that the ratio of bad actors who have infected legitimate servers versus those who have created bots on rogue virtual machines is shifting in favor of VM deployment. The flexibility to quickly spin up and take down VM instances as well as easily scale a deployment makes IaaS cloud computing a perfect fit for the dark trade.

The C2 Attack Landscape: Top Malicious Actors

Geographies with robust communications infrastructures remain fertile soil for C2s. These locations also happen to be in close global proximity to rich industrial and public sector targets for cybercriminals and rogue nation-state actors. It is important to note: the ultimate attack instigator may not be located in the same high-traffic geographies.

Top Attackers Span The Globe. In Q1, on average, the United States led all nations in generating C2 traffic. The United States has a wealth of infrastructure that lends itself to attack execution. Its proximity to valuable targets at home and abroad makes the United States a highly desirable location for criminals to establish a well-connected and stable control point.

TOP 10 COUNTRIES GENERATING C2 TRAFFIC GLOBALLY

1. United States
2. Ukraine
3. Russia
4. Netherlands
5. Germany
6. Turkey
7. France
8. United Kingdom
9. Vietnam
10. Romania

Source: Level 3℠ Threat Research Labs, Q1, 2015

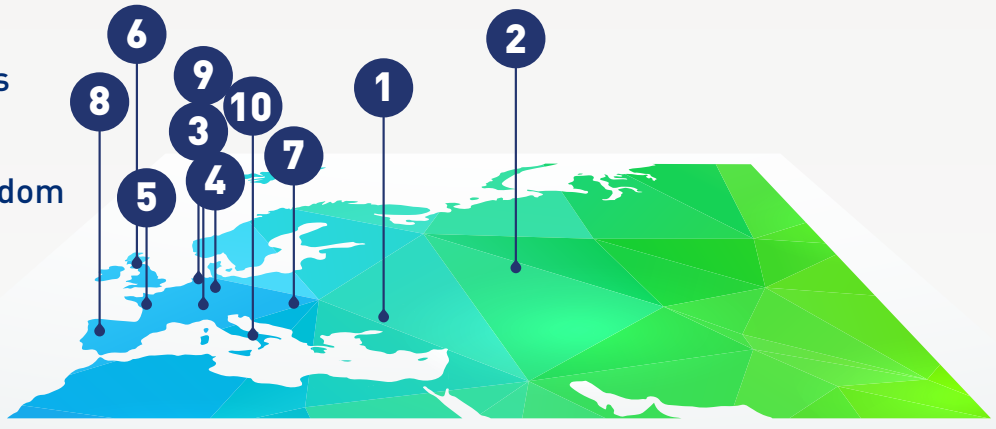
From a global perspective, the Netherlands ranked higher in relation to other countries in continental Europe. This top 10 spot is due to a large C2 and heavy port scanner claiming a number of victims in the Nordic region. The Netherlands affords a robust infrastructure, which makes it ideal for centralizing botnets for the region.

While nations around the world are represented in the top 10 global offenders list, the regions generating the highest levels of C2 traffic are Europe and the United States. An average of 20 percent of the C2s we tracked were based in North America with a nearly equal amount launching from the Ukraine and Russia combined. Western Europe[1] and the United Kingdom contributed another 12 percent of C2 traffic. Latin America was the source of only 2 percent of the overall C2 traffic.

Unusual communications to these countries should be automatic red flags for IT and security organizations. A review of whether servers should be communicating, authenticating or transferring data with endpoints in certain high-risk countries can be a predictor of potential threats to your environment or an indicator of a potential compromise.

TOP 10 COUNTRIES GENERATING C2 TRAFFIC IN EUROPE

1. Ukraine
2. Russia
3. Netherlands
4. Germany
5. France
6. United Kingdom
7. Romania
8. Spain
9. Switzerland
10. Italy

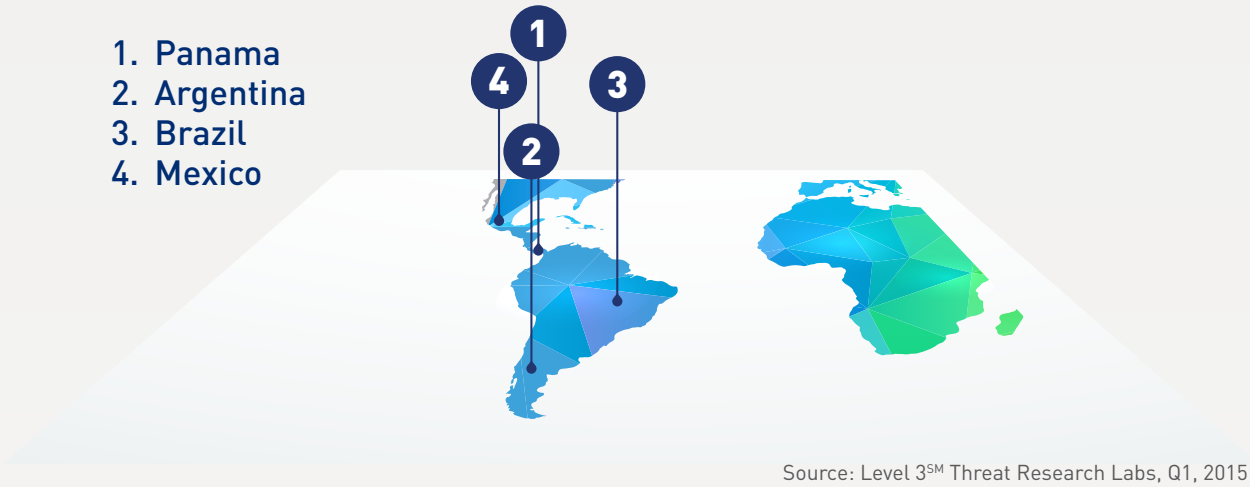


Source: Level 3℠ Threat Research Labs, Q1, 2015

1 Macro geographical composition is defined per 2013 United Nations Statistics Division.

TOP 4 COUNTRIES
GENERATING C2 TRAFFIC IN LATIN AMERICA

1. Panama
2. Argentina
3. Brazil
4. Mexico

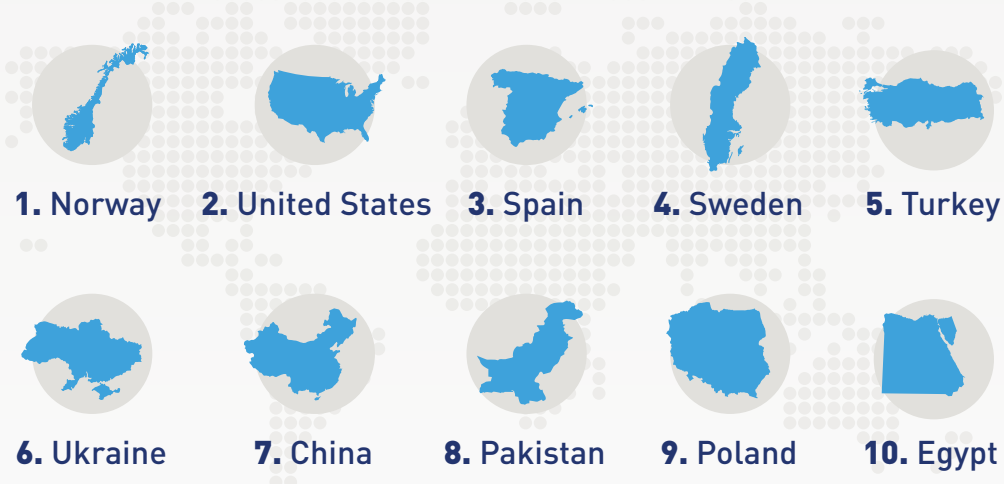


Source: Level 3℠ Threat Research Labs, Q1, 2015

Widespread Victimization

Who are the targets of these C2s and where are they located? In the first quarter of 2015, Norway received the most victim traffic across the globe. This may seem surprising both from a global and regional perspective. Norway's C2 volume was reflective of a C2 hosted within a specific Web hosting environment, which caused a sharp spike in identified C2 traffic. We see an over-balance of Nordic botnet communications with C2s — 22 percent of the global average of victim traffic. By comparison, UK victims comprised 2 percent and Southern Europe[2] comprised 11 percent of the global average. The high volume of attack traffic in the Netherlands correlates to the victim traffic in Norway and Sweden. Proximity to the target plays a large role in the efficacy of these campaigns.

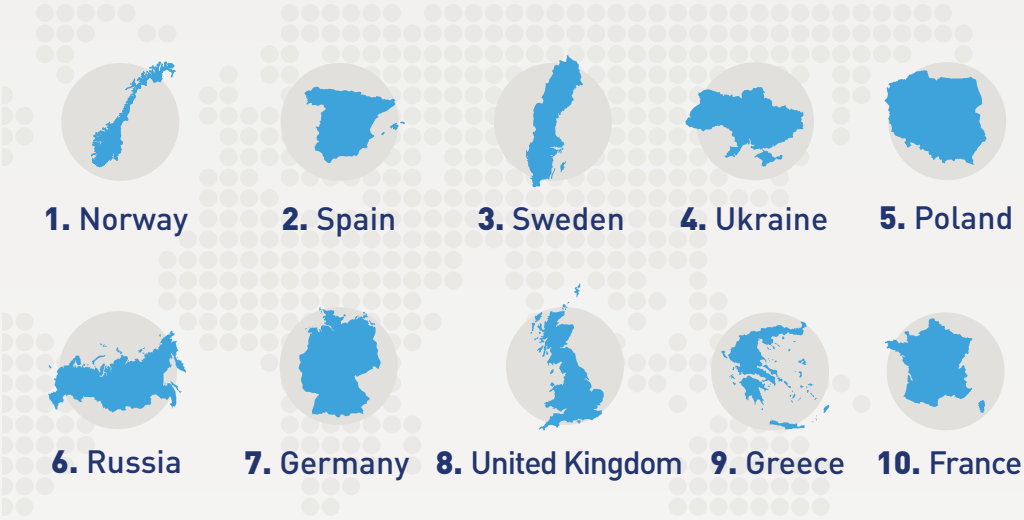
TOP 10 COUNTRIES
GLOBALLY COMMUNICATING WITH C2s



Source: Level 3℠ Threat Research Labs, Q1, 2015

2 Macro geographical composition is defined per 2013 United Nations Statistics Division.

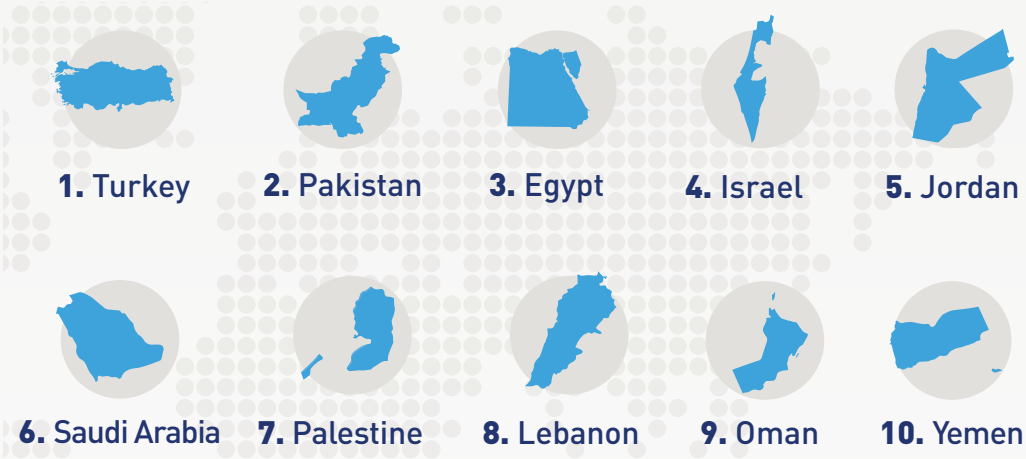
TOP 10 COUNTRIES IN EUROPE COMMUNICATING WITH C2s



Source: Level 3℠ Threat Research Labs, Q1, 2015

Countries in East and Southeast Asia were recipients of 7 percent of the global victim traffic, while those in Western, Central and Southern Asia drew 18 percent.

TOP 10 COUNTRIES IN ASIA (Western, Central, Southern) COMMUNICATING WITH C2s



Source: Level 3℠ Threat Research Labs, Q1, 2015

The Hardest Hit. During the course of the first quarter of 2015, the top five countries with the highest absolute number of victims, (unique IP addresses) conversing with C2s at a point in time during the quarter include:

- China – 532,000 unique-victim IP addresses
- United States – 528,000 unique-victim IP addresses
- Norway – 213,000 unique-victim IP addresses
- Spain –129,000 unique-victim IP addresses
- Ukraine – 124,000 unique-victim IP addresses

TOP 10 COUNTRIES IN ASIA (East, Southeast) COMMUNICATING WITH C2s

1. China **2.** Vietnam **3.** Taiwan **4.** South Korea **5.** Japan

6. Indonesia **7.** Thailand **8.** Philippines **9.** Malaysia **10.** Singapore

Source: Level 3℠ Threat Research Labs, Q1, 2015

TOP 10 COUNTRIES IN LATIN AMERICA COMMUNICATING WITH C2s

1. Brazil **2.** Argentina **3.** Mexico **4.** Venezuela **5.** Ecuador

6. Colombia **7.** Chile **8.** Peru **9.** Costa Rica **10.** Bolivia

Source: Level 3℠ Threat Research Labs, Q1, 2015

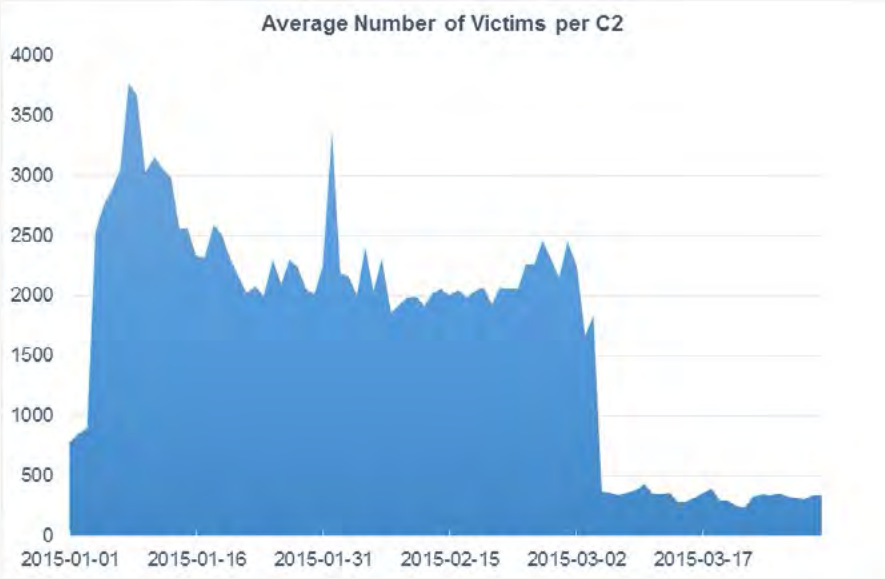
Given the large Internet-connected population in China and the United States, it is not a surprise that they are top targets. The United States has a sizeable number of heavily targeted private and public victims of interest to cybercriminals and malicious nation-state actors. Norway results are consistent with the large C2 event in the region. Latin America targets comprised 4 percent of the overall global average victim population due to its underdeveloped network infrastructure.

How Big Is A Botnet?

Average number of C2 victims
1,700
INFECTED HOSTS

According to our research, the average number of infected hosts per C2 is 1,700. Over the course of the year, we track 600 to 1,000 C2s, which control millions of infected hosts. The high volume of measureable communications between C2s and their victims suggest there is opportunity for the security community to collaborate and aggressively reduce the number of C2s on the Internet.

While this data may seem dire, when reviewed against day-to-day averages, botnet control measures used by the Internet security community and other commercial organizations are working overall. As the time graph demonstrates, the volume of victims per C2 declined over the quarter from a 3,763 peak in January to 338 in March, due to vigilance on behalf of the security community.



Source: Level 3℠ Threat Research Labs, Q1, 2015

The Botnet Market and Threat Diversification Trends

Botnets-for-hire is a big business. In the United States, access to 1,000 unique servers costs $190 a month[3]. Pricing has increased from 2013 where the price for the same service cost $20. Buyers in Europe have not seen the same steep

3 Dell SecureWorks, Underground Hacker Markets, December, 2014

22% of C2 servers have more than one THREAT PURPOSE

inclines, but pricing remains healthy. One thousand UK botnets costs about $120 USD per month[4]. The strong demand for botnet-as-a-service signals that bad actors see this as an effective method of attack. It also indicates that a trend of buying versus building is developing for the less sophisticated attacker. Level 3 Threat Research Labs found that 22 percent of C2 servers perform more than one function. Most likely, many of these botnets are commercial in nature, and they are part of a diversified business. For example, they may serve multiple, for-profit purposes, such as malware distribution, DDoS attacking and phishing services.

The good news for the security community is that commercial, multi-use platforms are most often built in a flat structure. While this configuration may be highly efficient for the botnet owner, it makes these operations easier for researchers to find, and for network operators to shut down. However, it would be naïve not to anticipate that these botnet operations would not reinvest their profits in more robust architectures to resist discovery. Botnet operation is a lucrative business with a simple setup. Operational costs to create, maintain and move a botnet, once shut down, are low. Blocked botnets can come back online often within hours of being shut down.

Tracking the threat purpose of a C2 is key because this data can serve as a predictor of risk. It is important to be able to determine if your servers are communicating with botnets that are operationalized to function in specific purposes, so that you can react to stop the threat. Mitigation may be as simple as blocking e-mail from these infected endpoints to prevent phishing, or it can mean something far more intricate to prevent infection.

Reducing Risk Through Botnet Control

Average age of a C2: **38 days**

Understanding characteristics of threat actors helps organizations and the security community manage the risks of today, and establish countermeasures. How are these tactics performing in the war against C2s? One of the methodolgies Level 3 uses to determine how well mitigations are performing is tracking the average age of a C2. The goal is to drive down the length of time C2s survive on the Internet, increasing the costs and burdens of operating a botnet. Our research shows the average age of a C2 for the first quarter of 2015 was 38 days, which has remained constant over the previous quarter. The expiration of a C2 can be caused on its own, a first-party takedown, or a third-party takedown. A first-party takedown refers to the situation where the owner of the host acting as a C2 discovers the infection and removes the malware. In some cases, the server owner can inadvertently break the malware's persistence by upgrading software or patching. In a third-party takedown, a service provider prevents connectivity between the C2 and the botnet either by blocking the DNS or IP addresses.

4 Ibid

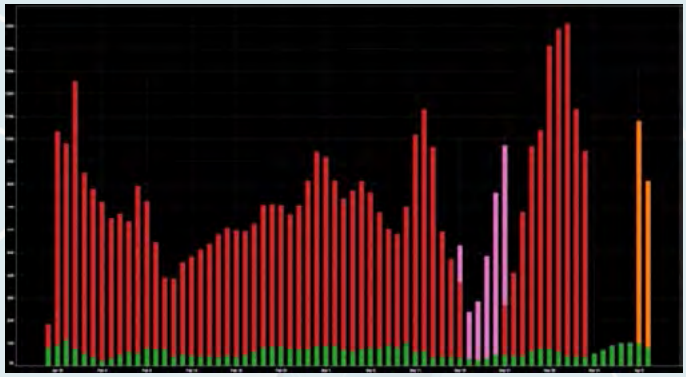
USE CASE

SSHPsychos: A Collaborative Approach to Botnet Control

In late March 2015, Level 3 began discussions with the Cisco Talos Group about working together to mitigate a Linux malware and rootkit used for DDoS attacks. This particular threat was documented in the September, 2014 Malware Must Die! blog and persisted more than four months later, when FireEye, a company that provides automated threat forensics, identified a large SSH brute force attack attempting to load the same malware. Cisco Talos Group continued tracking the threat and by the middle of the first quarter, Talos' honeypots saw more brute force authentication attempts from a single attacker than all other hosts combined.

Level 3's network data confirmed the massive scale this single attacker, now known as SSHPsychos, reached when compared with overall SSH Internet traffic. At times, this attacker accounted for more than 35 percent of total Internet SSH traffic.

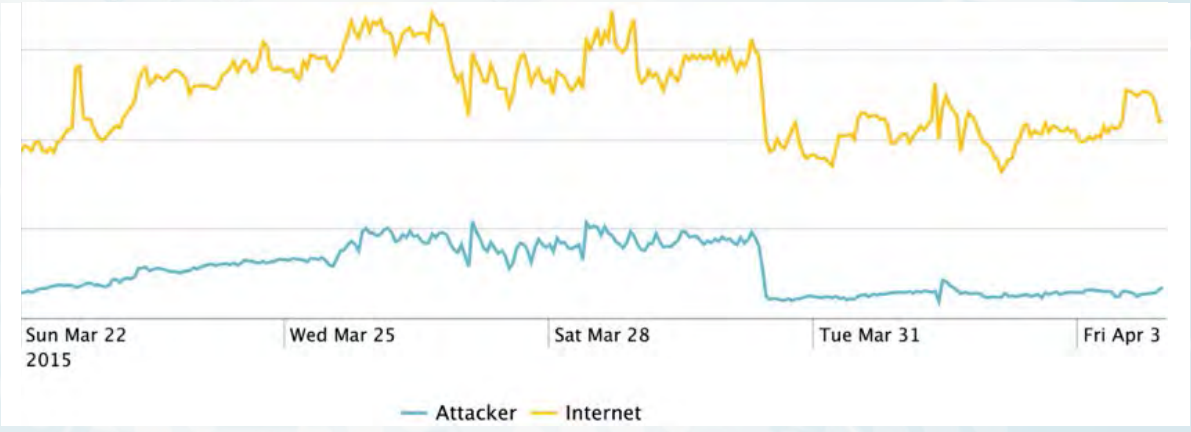
Over a two-week period in late March and early April, the Level 3 Threat Research Team monitored a large number of IPs scanned by the attackers, identifying which hosts in the Internet were active participants in the botnet. Upon validating the massive scale, impact and duration of this threat, they decided it was necessary to put our combined threat intelligence into action.



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

On April 7, after following proper protocols, Level 3 took action against SSHPsychos by blackholing all attacker traffic inside of our global network. This ensured that no traffic to the attacker would be sent through the Level 3 network. Outreach to other network operators included briefing them on the threat and formally requesting their participation in the permanent removal of the botnet from the global Internet.

Through the ongoing monitoring of the attacker's actions, the Threat Research Labs team observed the attacker changing it's SSH scanning operation domains with shifting multiple C2 and malware IPs. The team continues to monitor SSHPsychos behavior through its botnet algorithm analysis in the event the botnet attempts to resurface.



Source: Level 3℠ Threat Research Labs, Q1, 2015

End Goal

Our goal is to team with the security community to use our threat research and other sources of data to predict and detect bad actors on the Internet. Level 3 believes it is important to take an active and aggressive approach to reduce the life of C2s on the Intenet. Putting this belief into action, the team collaborated with Cisco Talos to pursue and take down the SSHPsychos botnet.

Mitigation Best Practices

For an in-depth technical profile of SSHPsychos, consult the Level 3 Threat Research Labs blog. Review IPs or hostnames mentioned in the article to ensure that you do not have any devices communicating with the attacker or participating in the botnet. Also included in the post are the current contents of the decoded malware file that can serve as a helpful source to find indicators of compromise from other attackers.

In general, if you have Linux machines running SSHD on the open Internet, be sure to follow the best practice of disabling root login in your –config file. That step alone would stop this particular attacker from being successful in your environment.

Consider adjustments in the way you run SSH daemon to avoid these types of attacks. Running a firewall locally on the Linux machine to protect against unknown access attempts is a strong step, when possible. However, when unsophisticated scans occur, you can even run SSH on a non-standard port as an avoidance method. Most commodity scanners and malware clients will not search for services on non-standard ports.

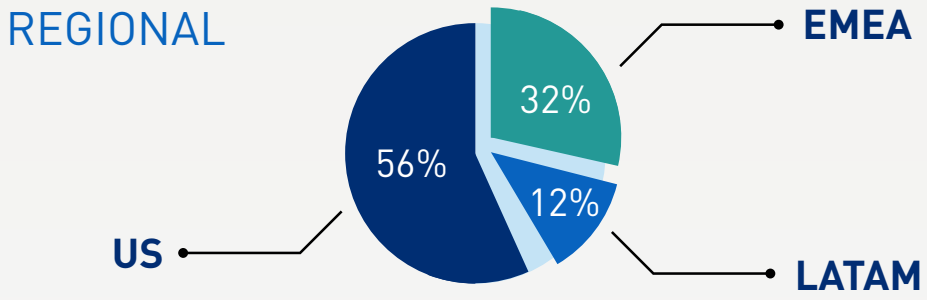
Validated system passwords have a minimal complexity requirement and common dictionary attacks are not effective against any user's password. To help protect against this problem, we have attached the passwords attempted by this attacker, as collected by Cisco's honeypots, to the blog. You can encrypt the list and compare to user passwords to help protect against potential attacks.

As a final measure, we always recommend monitoring DNS traffic traversing your networks for abnormalities. This particular malware hardcoded open resolver IPs that would have been an indicator to victims infected that something was abnormal within their environment.

Trend Alert: Denial of Service Attacks

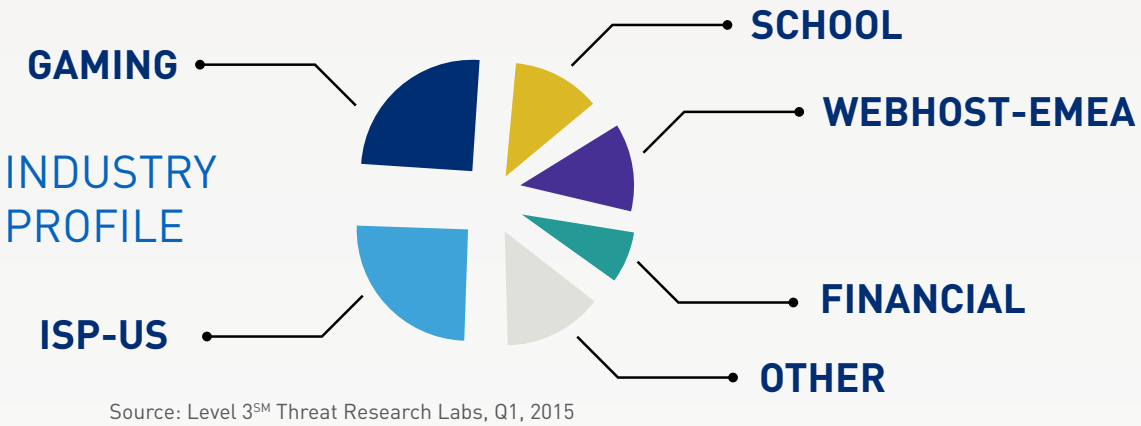
As we saw with SSHPsychos, once a botnet army is established, one of its purposes can be the DDoS attack. Over the past two years, both volumetric and application-layer attacks have increased in frequency. Blended attacks are also on the rise. DDoS attacks are effective when used with other forms of attacks meant to distract IT employees while inserting malware into backend systems to exfiltrate data.

Level 3 Threat Research Labs team analysis demonstrates the majority of attacks are aimed at targets in the United States, however DDoS attacks in Europe, specifically among those directed at Web hosting businesses, are trending up.



Source: Level 3℠ Threat Research Labs, Q1, 2015

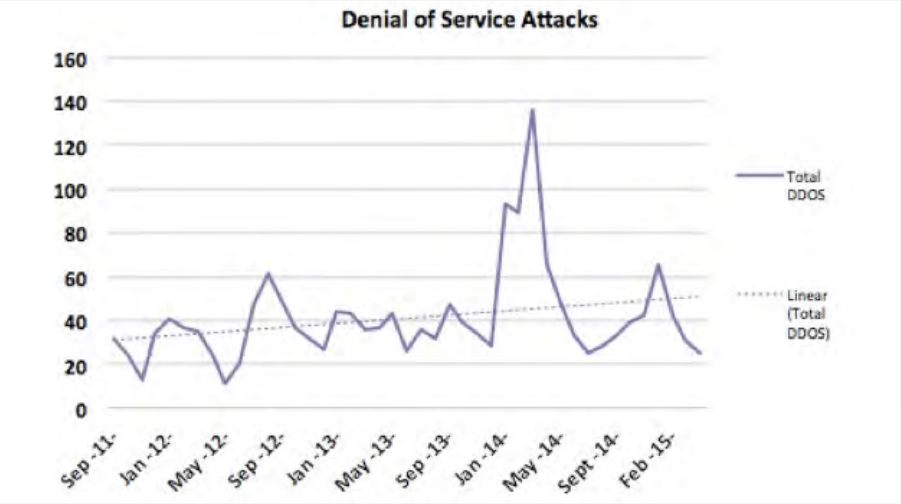
From a vertical perspective, the gaming industry, Internet service providers, Web hosting companies, research and education firms and the financial industry were the hardest hit in the first quarter of 2015.



Source: Level 3℠ Threat Research Labs, Q1, 2015

During the end of 2014 and into early 2015, Level 3 Security Operations teams saw DDoS attack volume spike after high-profile threats gained public attention and ignited copycat behavior. The sheer volume of attacks rose across the global Internet. Already considered one of the most affordable threats available for

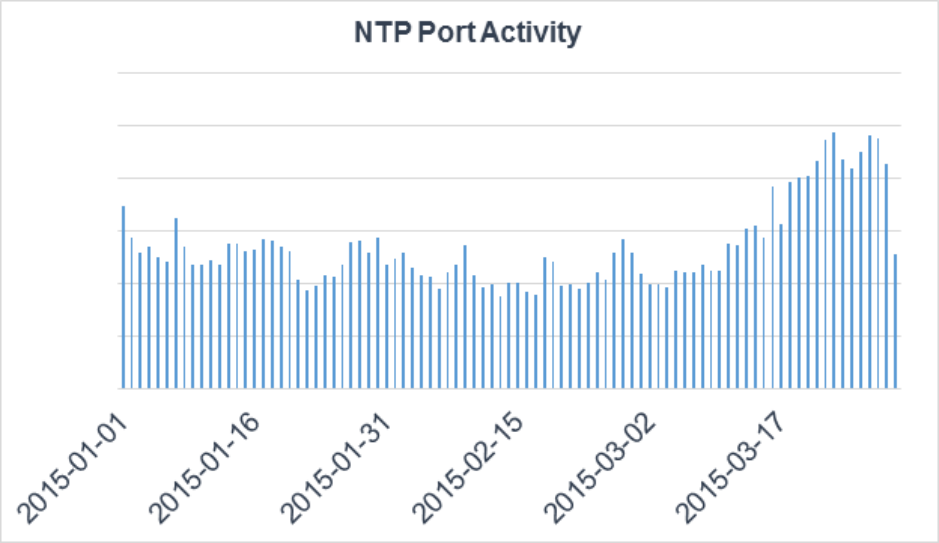
purchase on the darknet, popularity for the DDoS attack increased after the 2014 holiday season. A booter, or IP stressor, is an attack service that effectively rents out access to servers for a low, and usually monthly fee. The service is often offered by tiers based on the length of attack, from 100 seconds to 10,000 seconds. The highly publicized Lizard Squad enjoyed free product advertisement for its low cost DDoS-for-hire service Lizard Stressor, as it became widely reported upon in the popular press. For as little as $6 per month in bitcoins, the user can launch an attack of up to 125 Gbps for a period of 100 seconds. An unlimited attack capability cost $500 per month (all USD).



Source: Level 3℠ Threat Research Labs, Q1, 2015

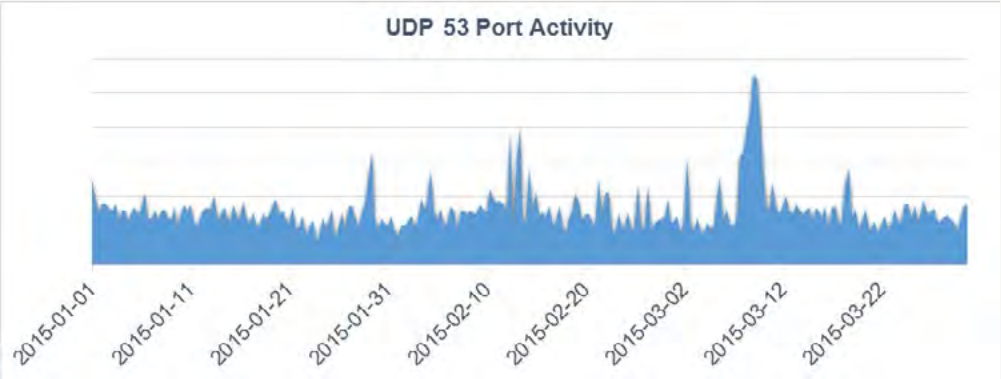
NTP Countermeasures Holding. In 2014, the Internet experienced a series of large-scale Network Time Protocol (NTP)-based amplification/reflection denial of service attacks. Since then, the Level 3 Security Operations team has been monitoring and reporting on this attack vector. NTP is the Network Time Protocol used to synchronize time with machines connected to the network on UDP port 123. At that time, the primary method of attack involved sending a valid NTP request (MON_GETLIST command) with the source IP address spoofed to match that of the target to NTP servers and forcing amplified response back to the targeted servers. Most valid users do not use the monlist command used in this specific reflective amplification attack. The command returns a list of the last 600 hosts that accessed the NTP server, resulting in a response multiple hundreds of times larger than the original request. At its peak, this attack resulted in additional attacks of amplification in the multiple hundreds of gigabytes in size. At of the end of the Q1, 2015 reporting period, NTP tracking indicators show that global mitigations implemented against this type of attack are holding. While some of the carriers are observing an increase in the NTP reflection amplification attacks, Level 3 has implemented constant NTP

DDoS attack countermeasures in its network. Consequently, the NTP reflection amplification attacks trendline specific to Level 3 does not have a meaningful change when compared to the past volume of NTP-based attacks for the period shown below.

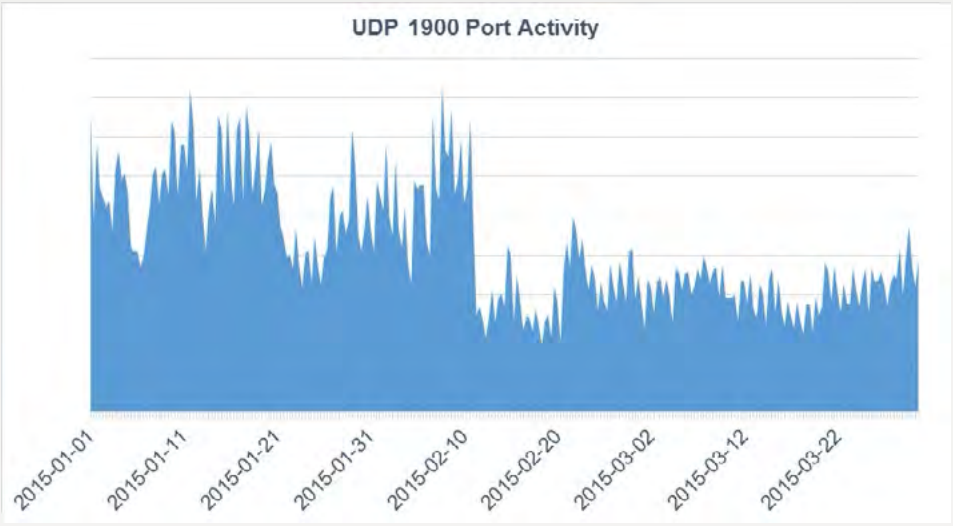


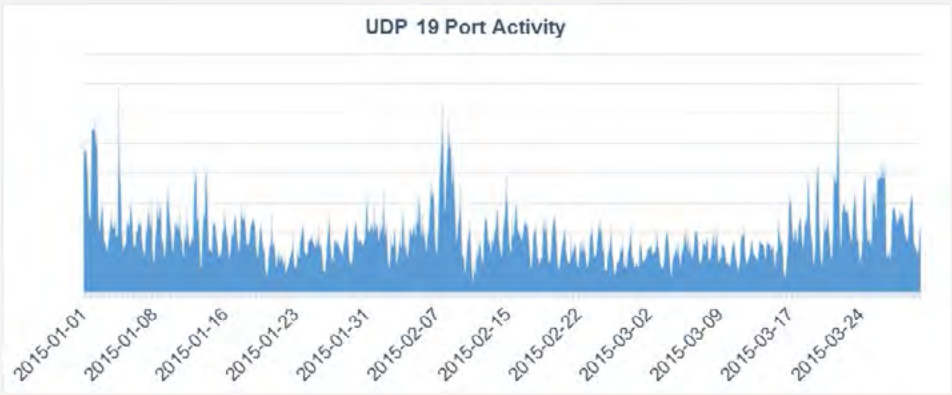
Source: Level 3℠ Threat Research Labs, Q1, 2015

In addition to NTP, some of the most common DDoS reflective amplification attack methods include DNS (UDP port 53), SSDP (UDP port 1900), and CHARGEN (UDP port 19). The charts below show the Level 3 Threat Research Labs analysis of the trends for that traffic across Level 3's infrastructure. It is reasonable to assume that the spikes above the average trend lines are related to reflective amplification attacks.



Source: Level 3℠ Threat Research Labs, Q1, 2015





Source: Level 3℠ Threat Research Labs, Q1, 2015

DDoS Threat Mitigation Best Practices

An effective DDoS mitigation strategy requires network-based, multi-layered defense with network controls, robust scrubbing capacity and threat intelligence. Implementing controls with your service provider such as Access Control Lists (ACL), rate limiting, and filtering on your Internet capacity can be a critical component to blocking threats. Such countermeasures can address a good portion of Layer 3 and 4 volumetric attacks. For example, if you serve solely HTTP and HTTPS traffic over your Internet link, you could use network-based ACLs to limit the impact of common volumetric attacks using NTP, SSDP, DNS, and others for its reflective surface.

The next layer of defense requires funneling traffic through network-based DDoS scrubbing centers. Like network controls, you can use DDoS scrubbing techniques to handle volumetric attacks, and provide an increased granularity in countermeasures over an ACL approach. Taken together, however, the two

approaches can be a powerful mitigation strategy. Prior to an attack, establish a baseline of healthy traffic characteristics. During an attack, traffic is routed to the scrubbers, "bad" traffic is filtered, and only "good" traffic is allowed to pass through to its destination. Ideally, DDoS scrubber deployments are regionally distributed to reduce latency that may occur due to rerouting. A high-availability, high-capacity ingest deployment is also critical to handle unpredictable traffic spikes. Scrubbing centers should be carrier-agnostic, meaning your provider should be able to scrub traffic regardless of the network IP address.

Threat intelligence can be the key to anticipating DDoS attacks as their botnets start to form across the Internet. High ingest capacity DDoS network controls, scrubbing platforms, as well as CDNs, can absorb brute force volumetric attacks. While spoofed volumetric attacks are still commonplace, DDoS mitigation platform capabilities must include functions to differentiate between advanced DDoS botnets and real users. Detection through challenge and response communications can identify botnets over real users. Today, there is a limit to this detection capability, as botnets are evolving to appear more like "real" computers on the Internet, exhibiting legitimate user behavior from their Web browser. This is why profiling, tracking, and blocking C2s is important. Strong knowledge of global infected endpoints can prove to be invaluable in mitigating sophisticated attacks.

Point of Sale Vulnerabilities: High Demand for Credit Card Data

The black market demand for user and credit card data has made retail system compromise a lucrative business. To cash in on this opportunity, malware manufacturers developed specialized software aimed at compromising the Point of Sale (PoS) system used by retail stores. This past March, Level 3 Threat Research Labs investigated an evolved malware strain and published its findings and actions taken to protect the Internet as a resource to the security community.

PoSeidon Take Down: Incident Overview

In late March, both Palo Alto and Cisco Talos released their findings on a new PoS malware FindPOS, based on honeypot intelligence. This malware, now known as PoSeidon, scrapes the credit card data found on compromised Microsoft Windows PoS systems, installs a key logger and then transmits captured data to exfiltration servers. The advantage to this process is that as soon as a shopper swipes his or her credit card on a compromised system, hackers can gain access to the data.

Hypothesis: Not long after this research was published, the known domains disappeared from the network. The teams posited that the mounting publicity forced the threat actor to change position. The Level 3 team tracked network traffic for the IP addresses associated with the malware domains and traced it through

DNSA record changes, as it is common practice for malware to be preconfigured with a set of domains and networks through which it cycles to avoid detection.

Behavior: Once the connection was reestablished with the C2s, the team observed that the infected system downloads a new binary that installs and executes a new process on the host. Among other actions, that FindPOS binary finds credit card data for exfiltration and captures PIN data with the logger. This flexible malware downloads and executes version updates and installs completely new malware packages.

Action: After following appropriate protocols, the Level 3 Threat Research Labs team executed a takedown of these control servers on our network.

Conclusion: The team continues to watch this strain carefully to help ensure that, as the botnet cycles through the pre-programed domains and network configurations, it does not resurface on the network. The team monitors these changes in an effort to minimize the botnet's impact on the Internet, and has communicated to other network service providers to do the same.

PoS Malware Best Practices

To gain a detailed technical understanding of how PoSeiden works, consult our Level 3 Threat Research Labs blog: Swipe At Your Own Risk: What you need to know to combat Point of Sale malware PoSeidon. This can help prepare your teams for the next malware variant.

PoS and support systems should be placed behind a properly configured firewall, with logs and alerts enabled, to the extent possible, for both ingress and egress traffic. A review of firewall logs for the presence of domains and IP addresses mentioned in our blog could enable location and isolation of compromised systems by PoSeidon. Adding in the logging of DNS look-ups to the hard-coded domains identified in the blog is recommended, as an additional layer of protection.

In this particular case, exfiltration takes place through port 80, which is generally used to access websites. You should lock down PoS firewalls to only allow traffic to known support sites on specific ports and disallowing all other port 80 traffic for this part of the network. Make sure the PoS device and other system software is up-to-date with the most current patches in place to close any known vulnerabilities.

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

Final Words and Recommendations

Threat intelligence data from network services providers can be effective against attackers if it is used by organizations to take action to protect networks, systems and data. To that end, IT security teams should consider the following:

- Investigate unusual communications between countries generating significant C2 traffic. A review of whether servers should be communicating, authenticating or transferring data with endpoints in certain high-risk countries can be a predictor of potential threats or a compromise.
- Organizations in Norway should stay on high alert for compromise, as the region was a primary target in late 2014 and early 2015.
- With 22 percent of C2s serving more than one threat purpose, evaluate whether activity such as port scanning may indicate greater risk to your organization.
- DDoS attack profiles, trends and mitigation solutions can help your organization stay in front of this mounting attack vector. Don't let these assaults become distractions from a more insidious attack objective that could be underway.
- Use the malware use cases detailed in the Level 3 Threat Research Labs blog to educate IT and security teams on complex threats and prepare for evolving attacks.

Level 3 believes it is critical that network service providers be proactive with their threat intelligence to remove threats, where practical, from the Internet. The team also believes organizations that arm themselves with available threat intelligence, including data from industry alliances and information-sharing organizations, are better able to defend against cyberattacks. Sharing threat data, and taking action with that intelligence, represents the new line of defense against threats to our information ecosystem and the enterprises they support.

ABOUT LEVEL 3

We build, operate and take end-to-end responsibility for the network solutions that connect you to the world. We put customers first and take ownership of reliability and security across our broad portfolio.

1.877.2LEVEL3
INFO@LEVEL3.COM
LEVEL3.COM