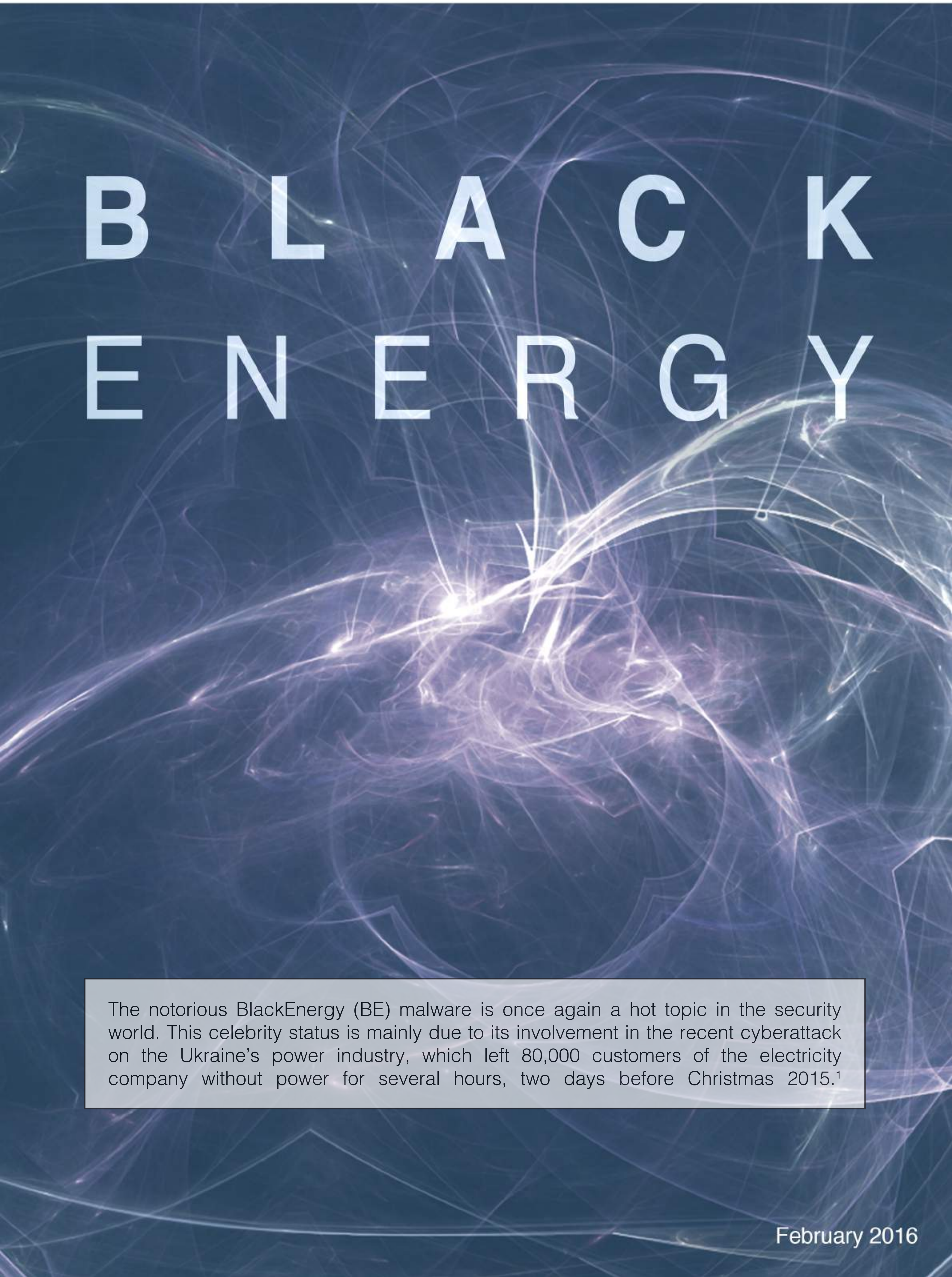
Security Report

ThreatSTOP



BLACK ENERGY

The notorious BlackEnergy (BE) malware is once again a hot topic in the security world. This celebrity status is mainly due to its involvement in the recent cyberattack on the Ukraine's power industry, which left 80,000 customers of the electricity company without power for several hours, two days before Christmas 2015.[1]

February 2016

Background

2007

Arbor Networks discovered the original BlackEnergy – a relatively simple HTTP DDoS Trojan – in mid-2007. During their initial research, Arbor Networks analyzed twenty-seven botnets infected by BE, with an estimated couple hundred bots in each network. Most of the botnets were in Russia and Malaysia, yet most of the top targets for the DDOS attacks were also in Russia, making the correlation between the attacked networks and the attacked sites unclear.[2] Since its first sighting, BE has taken many forms and has evolved into a sophisticated malware that can be used for fraud, spam, espionage, and targeted attacks.

2008

The first major attack in which BE was utilized was in 2008, when Russian hackers successfully hacked 54 communications, finance, and government websites in Georgia – just three weeks before the Russo-Georgian war. This attack is said to be the first case in history of a coordinated cyberspace domain attack synchronized with major combat actions in the other domains of war (consisting of land, air, sea, and space).[3]

2010

Later, in 2010 BlackEnergy was used in a massive cyber-fraud attack, this time with a newer version of the malware. BE v2 was better for the mission than its former counterpart, using plugins to carry out its various malicious activities. For example, in an event researched by SecureWorks, BE v2 took advantage of a plugin for a banking authentication system, which was used only by Ukranian and Russian banks, to steal authentication credentials. These credentials, as hypothesized by SecureWorks researchers, would be used to transfer money, and adjacently to launch DDOS attacks against the bank to distract them from noticing the fraudulent transfers.[4]

Background

2014

US Department of Homeland Security announced that the software responsible for running most of the nation’s critical infrastructure had been attacked with BlackEnergy, and had been infected since 2011. The compromised software was used to control oil and gas pipelines, power transmission grids, water distribution and filtration systems, wind turbines, and even nuclear plants. Had it gone undiscovered, this BE invasion could have seriously damaged US security and the country’s economy.[5]

Not only was 2014 a year of discovery for prior BE attacks that had gone unexposed, it was a year that brought many new samples to researchers’ attention. F-Secure labs went as far as stating that "The universe is full of BlackEnergy and so is cyberspace." In June, two BE samples were uploaded and researched by F-Secure Labs - one from Ukraine and the other from Belgium. A political party website in Ukraine had been a main target in the first attack, and Belgium is the home of the NATO headquarters. These facts, in light of the Ukranian political and national crisis peaking in 2014, raised speculation as to the motives of the attackers, and strengthened the notion that BE was being used mostly for political sabotage attacks. A few months later, ESET stated that they had been researching over one hundred individual victims of BE attacks that year, half in Ukraine and half in Poland, which included a number of state organizations and various businesses.[6]

2015

BE was used against several electrical distribution companies in Ukraine, peaking on December 23rd with the massive DDOS attack against the electrical power industry, leaving most of the Ivano-Frankivisk Oblast without power for six hours.

The sophistication that this bot has achieved over the years has earned it a high profile in the cyber world.

Infection Vector

The most common distribution method is as an email attachment. In a simple attachment-based infection, attackers attach an executable file (.exe) with the Word document icon to the malicious email, tricking victims into thinking it is a legitimate file.

Other methods take advantage of exploits in common programs. In one infection case, the attackers used a PowerPoint attachment, utilizing a vulnerability in the application that loads remote files in the background. In this way, the attackers were able to “silently” drop the malware dropper while showing a decoy document to the victim. Word (the well-known CVE-2014-1761 zero-day vulnerability), Java, TeamViewer and Juniper were also exploited for the use of infecting victims with BlackEnergy.[7]

World Wide Use Cases

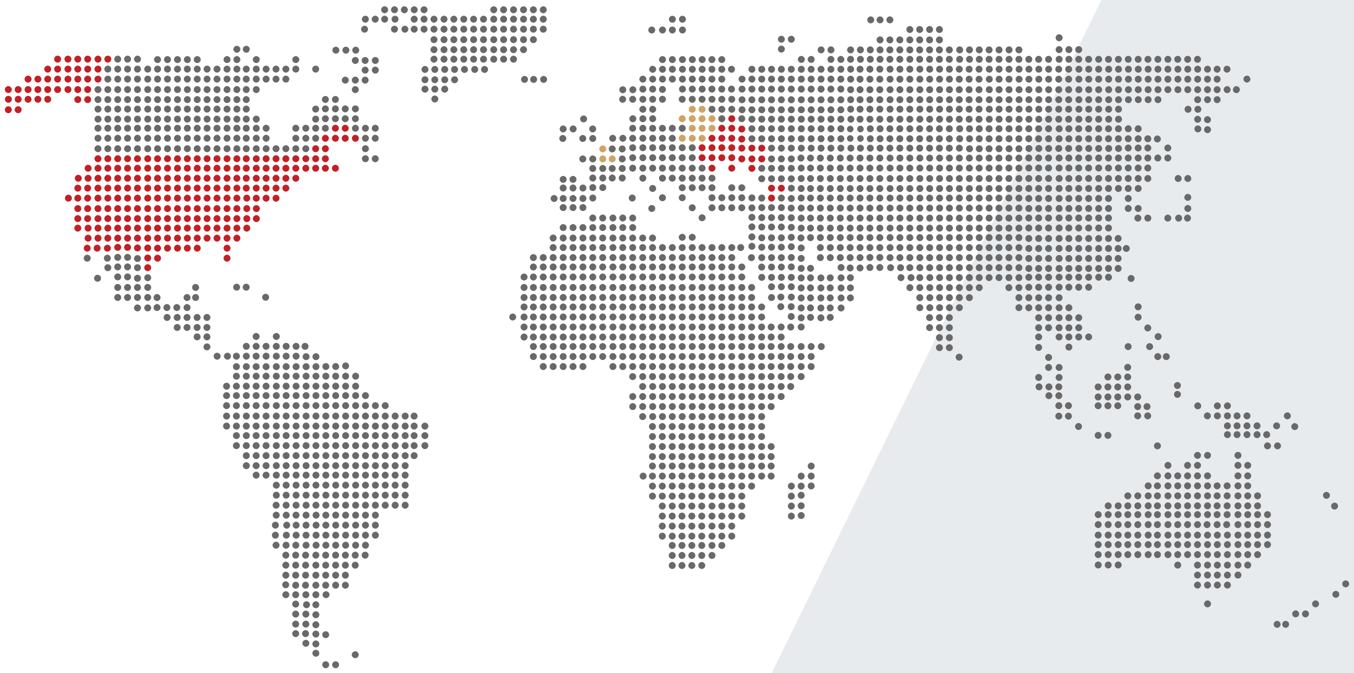
Energy[8]

Government

Finance[9]

Military[10]

Communication



BlackEnergy 1

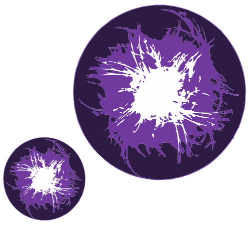
The first BlackEnergy samples researched by Arbor Networks in 2007 were of a web-distributed DDoS bot, used to target Russian sites while using Malaysian and Russian IP addresses.

Unlike most bots at the time, BE v1 did not communicate with the botnet master using IRC, nor did it perform exploit activities. Because of the lack of an exploit code, external tools and methods were necessary in order to load the bot.

The first version of BE had three distinct capabilities: DDoS attack commands, a download functionality using a “get” command to download from its servers, and commands to stop the bot from acting, such as “stop” (cease DDoS attacks), “wait” (act as a placeholder), and “die.” The bot’s way of evading detection was by hiding its processes and files in a system driver called “syssrv.sys.”

Russian underground hackers were said to be the owner of the bot, and although it was not widely available on the web, it was sold in Russian forums for computer hackers and in the Russian underground.[11]

BlackEnergy 2



After the big success of BE v1 came its second and more superior version, BE v2, which was publicly announced in 2010. The malware went through a complete code rewrite, and emerged with a modular architecture, making it easy to modify and suitable for spam, fraud and targeted attacks as well as its original DDoS functionality.[12]

The malware's flexible infrastructure utilizes plugins with various capabilities that can be downloaded and updated from the bot's Command and Control (C&C) servers. These plugins are saved in an encrypted format as drivers on the infected computer's hard drive.

Malicious plugins include the Trojan plugin, which can destroy an infected computer's entire filesystem when given a "kill" command, the DDoS plugin, as well as plugins used to gather user credentials, send spam, and more. In addition, the bot can download and execute remote files, execute local files, update itself from the C&C servers, and die on command.

The attackers' capability to easily update the bot on demand also makes the bot much more evasive – if the bot is discovered by an antivirus program, the programmers can simply write an update that overtakes the discovered part of the malware. The update is then sent to their bots for immediate action. This feature makes the bot's survival time on an infected computer much, much higher.[13]

BlackEnergy 3

The latest full version of BlackEnergy emerged in 2014. The changes made to this version were smaller, mainly simplifying the malware. For instance, the v3 installer does not use a driver component in the installation process, as did the previous versions, but rather the installer drops the main DLL component directly to the local application data folder.

Another modification made to v3 is that it communicates with its plugins using a different protocol than its predecessors.[14]

BlackEnergy Lite

Also called “BlackEnergy Mini”, this version runs its plugin capabilities differently and with less support than its “big” counterparts and leaves a lighter footprint. BE Lite’s configuration files are stored as a x.509 certificate (responsible for public key verification), instead of as an XML file like the other versions of the malware.[15]

Main Actor: SandWorm

The most prominent use of BlackEnergy for targeted attacks is by a cyber gang who is attributed to Russia. The group, who was named Sandworm because of the references to the science-fiction series "Dune" embedded in their malware,[16] was researched mainly from late 2013 and throughout 2014, and it seems that the team's activity traces back to 2009. The group's preferred infection tactic is spear phishing, and they use BE v3 as their signature malware.

The Sandworm team is known to have a particular interest in political targets, and is said to be responsible for the 2014 attacks against Ukranian government organizations. Other organizations the gang has targeted include NATO, Western European government organizations, Energy Sector firms, European telecommunications firms, and American academic organizations.[17]
In addition, it is suspected that Sandworm was involved in the 2008 attack on Georgia.[18] Many tie Sandworm to the Russian government, though there is no proof of any connection.

Most mainstream media outlets have quoted the security firm iSight, who claims that Sandworm is responsible for the recent Ukranian power outage.[19] This is probably largely due to the fact that BlackEnergy v3 was found in the samples uploaded from the attack, as well as the political motive of the group. Others say this is a loose assumption and is not adequate evidence to tie the cyber gang to the attack.

BlackEnergy has been, and will probably continue to be, an extremely powerful and intriguing malware researched by the biggest security companies today. ThreatSTOP has been actively analyzing indicators for this malware, and is currently protecting its customers from the malware by blocking any potential traffic from their network to BE's C&C servers.

References

[1] http://www.bbc.com/news/technology-35297464

[2] http://atlas-public.ec2.arbor.net/docs/BlackEnergy+DDoS+Bot+Analysis.pdf

[3] http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf

[4] http://www.eweek.com/c/a/Security/Russian-Banking-Trojan-BlackEnergy-2- Unmasked-at-RSA-883053

[5] http://abcnews.go.com/US/trojan-horse-bug-lurking-vital-us-computers-2011/story?id=26737476

[6] https://www.f-secure.com/weblog/archives/00002721.html

[7] http://www.welivesecurity.com/2014/10/14/cve-2014-4114-details-august-blackenergy-powerpoint-campaigns/

[8] http://www.theregister.co.uk/2016/01/04/blackenergy_drains_files_from_ukraine_media_energy_organisations/

[9] http://www.eweek.com/c/a/Security/Russian-Banking-Trojan-BlackEnergy-2-Unmasked-at-RSA-883053

[10] http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf

[11] http://atlas-public.ec2.arbor.net/docs/BlackEnergy+DDoS+Bot+Analysis.pdf

[12] https://www.virusbtn.com/conference/vb2014/abstracts/LM3-LipovskyCherepanov.xml

[13] https://threatpost.com/inside-blavck-energy-2-botnet-072110/74236/

[14] https://www.f-secure.com/documents/996508/1030745/blackenergy_whitepaper.pdf

[15] https://www.virusbtn.com/conference/vb2014/abstracts/LM3-LipovskyCherepanov.xml

[16] http://www.reuters.com/article/us-ukraine-cybersecurity-sandworm-idUSKBN0UM00N20160108

[17] http://www.isightpartners.com/2014/10/cve-2014-4114/

[18] http://www.securityweek.com/blackenergy-malware-linked-targeted-attacks

[19] http://www.reuters.com/article/us-ukraine-cybersecurity-sandworm-idUSKBN0UM00N20160108

ThreatSTOP®

www.threatstop.com

Block inbound attacks and prevent data theft.

Key benefits:

- Automatically delivers the latest actionable threat intelligence to network devices and DNS servers based upon user-defined policies.
- Proactively deflects inbound malware, DDoS and other attacks, regardless of the attack type or vulnerability. Renders your network invisible to scanners, so attackers move on.
- Prevents data theft and corruption by stopping malware from "phoning home" to threat actors. Prevents activation of ransomware such as Cryptowall and Cryptolocker.
- Cloud-based service is easy to manage and provides protection using your existing hardware. Works with leading firewalls, routers and switches.

Powerful Security without Complexity

Automated, actionable threat intelligence

Your organization is under constant surveillance by threat actors looking for gaps in your security posture. Automated scanners actively seek out open ports to gain access to your network, while employees pick up malware from infected websites and phishing emails. You have invested in a battery of overlapping security tools, yet the breaches continue.

Make it stop. ThreatSTOP Shield is a powerful service that blocks attacks before they reach your network, and prevents data theft. Unlike other tools that only integrate into a SIEM or notify you of threats, ThreatSTOP deflects attacks that have bypassed your firewall, IDS/IPS, web filter and endpoint security. Then ThreatSTOP's real-time reporting provides the visibility you need to remediate threats.

Service Overview:

ThreatSTOP Shield is a highly effective, proactive security solution that blocks advanced threats. It delivers up-to-the-minute protection against malware, DDoS and other advanced attacks, and enhances your existing security posture by improving the effectiveness of firewalls, IDS/IPS, routers, switches, endpoint and other security tools.

The service protects your network and devices by automatically delivering best-in-class threat intelligence to your perimeter security devices, including firewalls, routers and switches. A cloud-based service, it is easy to deploy and manage, and does not require upgrades to your infrastructure or new hardware. Once deployed, ThreatSTOP Shield provides immediate relief by deflecting attacks and unwanted or malicious traffic.

Best-in-Class Threat Intelligence

ThreatSTOP Shield leverages the company's comprehensive and authoritative database of IP addresses, domains and the infrastructure used for cyberattacks. When selecting a threat intelligence service, it is not the size of the database, but accuracy that is important. ThreatSTOP's world-class security team curates the latest threat information and cross-correlates threat data against multiple public and private sources to ensure a high degree of accuracy and prevent false positives.

How it Works

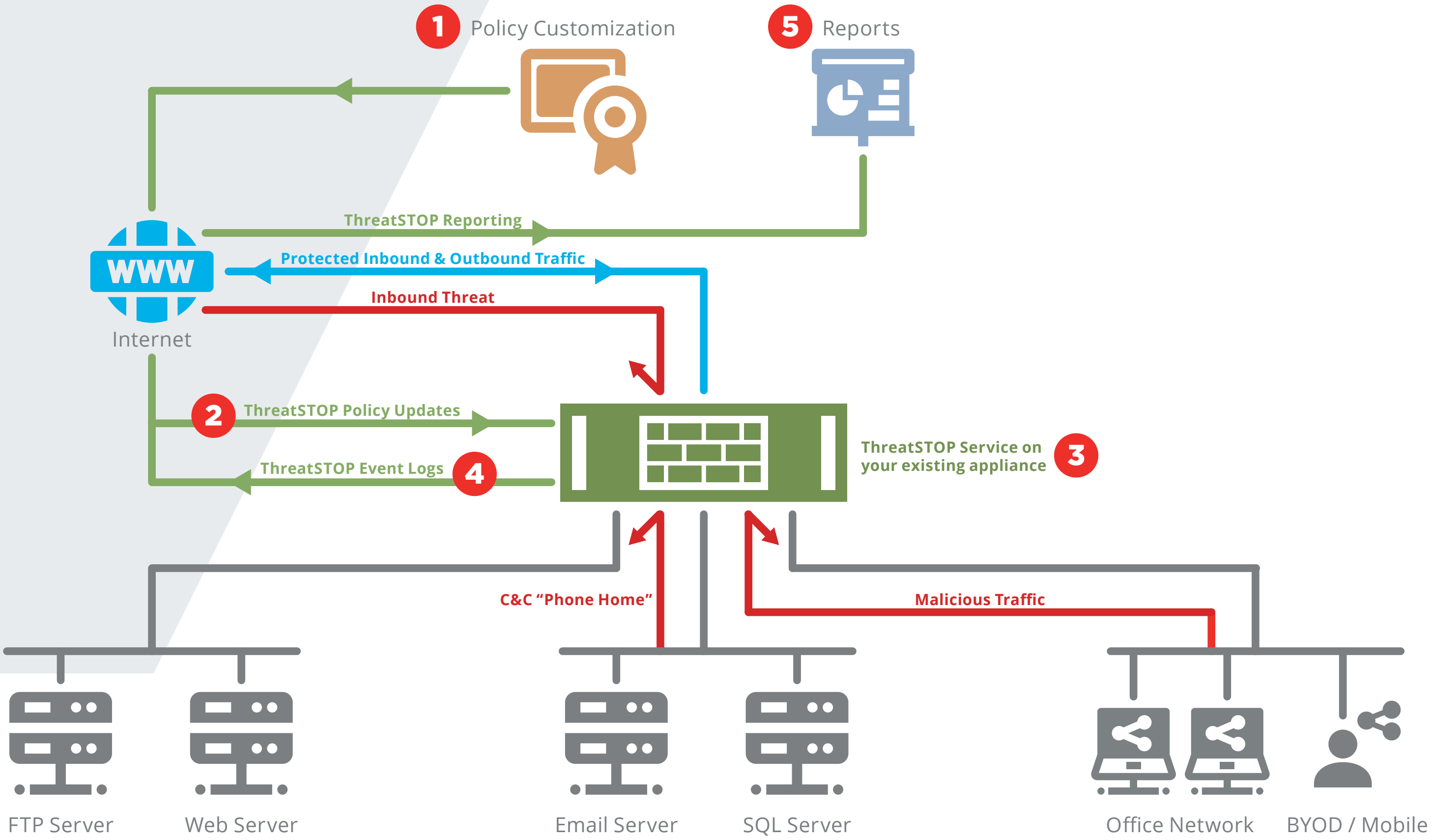
Step 1 Select from expertly-crafted threat protection policies, tailor a perfect fit by creating your own whitelists and blocklists.

Step 2 Policy updates are sent automatically to your appliance containing up-to-the-minute threat intelligence to protect against current threats.

Step 3 Devices can now enforce those policies to protect your network from inbound attacks and outbound malicious connections.

Step 4 Event logs are generated providing visibility into the traffic that was blocked prior to reaching your network.

Step 5 View powerful reports about the threats targeting your environment, and details of potentially infected devices to expedite remediation.



Additional benefits:

Scales to protect network of all sizes

As a broad-based solution that leverages DNS to protect every device connected to your network, it can protect any network, from virtual cloud networks to branch LANs to the largest carrier networks. It protects all devices, any port, any protocol and any application.

World-class hosting, reliability and performance

The service is operated across multiple world-class flagship data centers offering N+1 or better redundancy on all systems. Through implementation of anycast network technology, customers are ensured higher availability and resilience against brute force attacks. With audited security protocols, the service meets the international service organization reporting standard SSAE 16 for SOC 1, 2 and 3, Type II reports.

ThreatSTOP provides essential security to manage risk, offering broad protection for your environment that protects all devices from attack and prevents data theft. To request a demo or speak with a salesperson, please contact **sales@threatstop.com** or call **760 542 1550**. Visit www.threatstop.com for more information.