The Shadowserver Foundation

What Is Shadowserver?

The Shadowserver Foundation is an altruistic not-for-profit organization (NPO) working to make the Internet more secure for everyone. We have unique sources, a global vantage point and partnerships with National Computer Security Incident Response Teams (CSIRTs), Law Enforcement, industry and security researchers world-wide. We work collaboratively and share information with Internet defenders at no cost to mitigate vulnerabilities, detect malicious activity and counter emerging threats.

Our unparalleled combination of position, trusted information and 18 years of proven community partnerships enables Shadowserver to perform a critical role in Internet security.

Our Mission

Our mission is to make the Internet more secure by bringing to light vulnerabilities, malicious activity and emerging threats. We are driven by the vision of a secure, threat-free Internet.

What We Do

Shadowserver delivers free, high-quality, actionable, cyber threat intelligence to Internet defenders globally.

Our team of passionate subject matter experts are trusted by third party cyber incident responders to provide timely data and valuable insight, helping Internet defenders more effectively secure their networks and better protect victims of cybercrime. Our public benefit services help build cyber security capability worldwide, increasing the overall resilience and security of the Internet for everyone.

Benefits to Society

Over 7000 organizations globally make use of our free data feeds every day. We work with businesses, from SMEs through to the largest enterprises (including many Fortune 500 companies), to improve network security, enhance their product capability, and advance threat research. We enable financial institutions, health services, education providers, network operators, ISPs and hosting companies to better protect their systems and users.

We partner with law enforcement to help prevent cyber attacks and take down cybercrime infrastructure around the world, or identify, protect and notify victims so that they can be remediated.

Shadowserver helps 201 National CSIRTs in 175 countries and territories to understand both the big picture and the low-level, daily details of what is happening on the networks they are responsible for, including critical national infrastructure. This improves situational awareness and allows them to better detect, track and respond to new threats targeting their countries.

We support academic institutions and corporate or independent researchers in groundbreaking cyber security research. We also help policy makers make more informed cyber security decisions. Our work enables individual private citizens to interact globally through a safer and more secure Internet.

Shadowserver collaborates with a wide range of organizations internationally to raise security

awareness, conduct outreach, build capacity, enhance defensive capabilities, and provide education and mentoring - particularly in developing nations. We actively promote a culture of responsible sharing, establishing mutual trust and strong collaborations. We run successful initiatives and services that achieve community benefits for all Internet users. Improving the security of each individual network collectively makes the whole Internet more secure.

Global Operations

We are a world leading, highly specialized cyber security NPO. Our public benefit services have operated 24/7 at full Internet scale for 18 years. Highlights include:

- Scanning all 4.2 billion IPv4 and over one billion IPv6 addresses on multiple ports every day - identifying misconfigured or abusable devices before they are targeted by attackers and notifying owners about compromised devices on their networks.
- Disrupting criminal control of malware infected computers, by sinkholing billions of connections from hundreds of different botnets. This enables us to report millions of unique victim IP addresses per day to network owners for timely remediation.
- Collecting hundreds of thousands of new malware samples every day, as well as periodically re-analyzing our entire repository of over 1.7 billion samples. We perform extensive technical analysis on each sample and map out the associated criminal command and control infrastructure in order to aid cybercrime disruption efforts.

Shadowserver has a range of unique capabilities. We collaborate closely with partners to generate successful global impacts and achieve positive outcomes in the ongoing fight against cybercrime. We have played a critical, behind-the-scenes role in many of the largest anti-cybercrime actions over the past decade, supporting our partners with cutting edge technical capabilities, investigative assistance and victim notification channels. This includes high profile 2021/2022 incidents such as Solarwinds SUNBURST, Microsoft Exchange Servers compromised by the HAFNIUM APT group and other threat actors, the 21nails open source mail server vulnerabilities, Apache Log4j exploitation, Emotet botnet victim remediation and record breaking Mitel TP240 reflected amplification DDoS vector remediation. We also recently participated in regional capacity building outreach campaigns in Africa and the Indo-Pacific. We are a founding member of the Ransomware Task Force and a member of the NoMoreRansom initiative.

All of this activity depends on hundreds of servers, petabytes of storage, complex technology stacks and an agile, highly skilled team of dedicated and motivated individuals. We operate an extensive data center facility in California, as well as from locations across the US and Europe, and sensors globally. Our 2022/2023 Alliance fundraising target is USD $3,200,000.

How Shadowserver Is Funded

Our shared successes have been made possible by funding in the form of grants, sponsorship and donations from organizations who value the public benefit services Shadowserver provides for free to the whole Internet.

Tax Deductible Donations

The Shadowserver Foundation is registered as a tax-exempt 501c3 corporation in the USA and a Stichting (foundation) with ANBI public benefit status in the Netherlands. Donations to our US and NL legal entities are effective tax deductible impact investments for corporate and individual donors.

The New Shadowserver Alliance

From October 2022, **The Shadowserver Alliance** became the new primary vehicle for ensuring our long term sustainability as a provider of free, public benefit services. **Our mission is not changing: we will always remain a not-for-profit entity passionately committed to providing essential data and services to our constituents for free.**

At a time when traditional security boundaries have been stretched by increased working from home during the global COVID-19 pandemic, **we are actively seeking new Shadowserver Alliance Partners** to join us now in the next phase of our journey. As a strong community, we can continue to raise the bar on cyber security globally together.

Trusted by Experts Globally

Mastercard: "*We are proud to act as ambassadors for their mission. Our hope is that through our partnership, more organizations and companies will take advantage of the valuable information they provide. By collectively sharing insights, we can build a safer digital ecosystem, one that supports the digital economy working for everyone, everywhere*" (link)

Trend Micro: "*one of the world's leading resources for reporting vulnerabilities, threats and malicious activity … our shared digital world is a safer place today because of their efforts … their work has helped to pioneer a more collaborative approach among the international cybersecurity community, from vendors and academia to governments and law enforcement*" (link)

AVAST: "*Shadowserver works together with industry sectors, national CSIRTS, and law enforcement agencies, such as the FBI, Interpol and Europol, providing access to invaluable critical data*" (link)

FBI: "*That herculean effort included contributions by investigators in more than 40 jurisdictions, Europol, the Shadowserver Foundation, a German research institute, ICANN, national CERTs, and domain registries around the world … We've got to take an enterprise approach—one that involves government agencies, private industry, researchers, and nonprofits, across the U.S. and around the world*" (link)

"***Europol's European Cybercrime Center (EC3)** is very pleased to team up with The Shadowserver Foundation to counter cybercrime, as it threatens the safe use of the Internet by people around the globe. The cooperation will enhance our ability to inform and help people who are victims of cybercriminals, and will strengthen our combined efforts in mitigating the damage done by malware and other forms of cybercrime*" (link)

The Internet Society: ""*The internet depends upon voluntary, collective action to make us all secure" Internet Society president and CEO Andrew Sullivan said in a statement. "Shadowserver's approach gives every network operator the tools to improve their own network security. It's the way to make sure the internet is secure and trustworthy for everyone"*" (link)

European Commission: "*The non-profit organisation Shadowserver contributes to a safer Internet worldwide*" … "*The provided scheme of information is assessed as highly valuable*" … "*conservation of Shadowserver services is of high importance to the community*" (link)

"***CERT-Bund (Germany)** very much appreciate the awesome and tireless hard work Shadowserver has been doing to support the international security community for many years. The daily reports on malware infections and open accessible services provided by Shadowserver to national CSIRTs feature a valuable, high-quality resource of information for identification of security issues and notification of effected parties*" (link)

CERT.at (Austria): "*The Shadowserver Foundation is not only the largest source of threat intelligence worldwide, it is also by far the most important source of information for CERT.at on topics such as malware infections, vulnerable systems*" … "*The quality of the data made available in this way is far superior to that of most others, even though it is made available completely free of charge*" … "*If you have budget left over in your business, this is surely one of the best ways to use it - all of the internet will thank you for it*" (link)

Asia Pacific APNIC: "*unsung hero [that keeps the] internet secure*" … "*key to the success of this community for a long time*" (link)

WIRED: "*Shadowserver has a vital behind-the-scenes role; it identifies online attacks and wrests control of the infrastructure behind them … Shadowserver has quietly worked on numerous facets of internet security since 2005* … [and had] *consistent involvement in crucial security operations*" (link)

WIRED: *"KEEPING THE INTERNET safe may sometimes feel like a game of Whac-A-Mole, reacting to attacks as they arise, then moving on to the next. In reality, though, it's an ongoing process that involves not just identifying threats but grabbing and retaining control of the infrastructure behind them. For years a small nonprofit called Shadowserver has quietly carried out a surprisingly large portion of that work … A critical internet safeguard … Shadowserver has helped keep the internet safe for 15 years … Think of Shadowserver as the internet's protection grid*" (link)

Brian Krebs (krebsonsecurity): "*Ghostbusters … The Web's Bot Containment Unit … the trusted partner when national law enforcement agencies needed someone to manage the technical side of things*" (link)

CNN: "*The [Dridex] botnet is now under the control of an organization called The Shadowserver Foundation, a little-known group of professional hackers who volunteer to make the Internet safer for the public*" (link)

CNN: **""***The FBI-controlled server will capture the IP addresses of [VPNFilter] affected devices and a private-sector partner group, The Shadowserver Foundation, will work to scrub and restore them", the Justice Department said*" (link)

BBC: "*The Shadowserver Foundation is a group of security professionals who volunteer their time to track and measure botnets to help law enforcement investigations*" (link)

Bankinfosecurity: "*Botnet designed to mine virtual currency shut down … ESET is working with … the nonprofit Shadowserver Foundation, which researches and tracks botnets, to notify victims and help clean devices of the VictoryGate malware*" (link)

Input Magazine: "*The internet has a lot of underlying infrastructure most of us seldom give much thought to, but which is essential to keeping it working... and working properly. One of those seldom-seen, essential services that works tirelessly to keep things running smoothly is a nonprofit called Shadowserver*" (link)