2018 Whitepaper

Dome Shield

Threat Intelligence

COMODO
CYBERSECURITY

Comodo Security Solutions, Inc.
1255 Broad Street
Clifton, NJ 07013
United States
Tel: +1 (877) 712 1309
Tel: +1 (888) 551 1531
Fax: +1 (973) 777 4394
Inquire: sales@comodo.com
Support: c1-support@comodo.com

DELIVERING AN INNOVATIVE CYBERSECURITY PLATFORM TO RENDER MALWARE HARMLESS

The Comodo Threat Research Labs (CTRL or "the Lab") pursues a mission to use the best combination of cybersecurity technology and innovations, machine learning-powered analytics, artificial intelligence, and human experts and insights to secure and protect Comodo customers, business and public sector partners, and the larger end-user community.

The Lab monitors, filters and contains, and analyzes malware, ransomware, viruses and other unknown thereby potentially dangerous files 24x7x365 encountered in 190 countries around the world. With five offices across the Americas, Asia, and Europe, the Lab employs more than 120 IT security professionals, ethical hackers, computer scientists and engineers – all full-time Comodo employees. CTRL staff analyzes millions of potential pieces of malware – components of phishing, spam or other malicious/unwanted files, attached to emails or downloaded from websites – every day. The Lab also works with trusted partners in academia, government and industry to gain additional insight into known and potential threats.

COMODO Dome Shield and Threat Intelligence

Comodo Dome Shield is a cloud-delivered DNS-based Security-as-a-Service (SaaS) solution that provides comprehensive domain filtering and granular policies that cover security and category-based rules. Comodo Dome Shield blocks over a half million threats and malicious attempts daily by building on threat intelligence derived from Comodo global presence and aggregated and analyzed by the Comodo Threat Intelligence Lab.

Comodo Dome Shield protects against a range of threats and attack types:

Bots and Botnets

Botnets are comprised of hundreds, sometimes thousands of internet-connected devices compromised by hackers, viruses or trojan horses, supervised by a command-and-control (C&C) server. Botnets are often used for DDoS attacks, E-mail spamming, cryptocurrency mining and other distributed malware applications. Comodo Dome Shield is highly effective at discovering botnet members by analyzing network communication of unknown files, detection of processes that exchange data with known C&C host, and recognition of communication patterns characteristic of botnet member behavior.

You can block botnet members by selecting **Botnet/C2C/Bot Infected Sources** in Comodo Dome Shield security rules.

C&C Hosting

Command-and-Control servers (C&C or C2) are used by attackers and malware authors to control compromised hosts through various network communications. Compromised hosts are mostly malware-infected, often aggregated into botnets. Attackers both maintain lists of active compromised hosts (botnets) using heartbeats and issue commands to execute targeted attacks using these botnets. Detailed malware behavior analysis inside Malware Zoo makes it possible to discover known / Zero-Day C&C hosts.

You can block C&C Sources by selecting **Botnet/C2C/Bot Infected Sources** in Comodo Dome Shield security rules.

Compromised or Hostile Servers

These machines include hosts used by hackers for malicious activities and/or sites infected with malware that could host botnet software, Command-and-Control servers and spamming mail servers.

Drop Sites

Drop Sites enable hackers to collect, distribute and sell information exfiltrated from hacked systems on the Dark Web and on underground markets. Drop sites typically contain passwords harvested by keyloggers, sensitive information collected by ransomware and other stolen data, uploaded for further actions.

Malware Domains

Malware hosting servers are employed to distribute malicious files in multiple ways, such as supplying fake official setup files, or served for use by other malware, by allowing direct access to the file resource.

You can block access to Hostile Servers, Drop Sites and **Malware Domains** by selecting Malware Domains in Comodo Dome Shield security rules.

Phishing

Black hats send phishing emails to corporate employees and home users to direct them to deceptive web sites or to download and run malicious executables. Sites leveraged for phishing use automatically generated e-mail addresses to originate phishing attacks, most often time targeting organizations hosting commercially or strategically valuable with the goal of exfiltration and remuneration. Phishing emails often appear to originate from a legitimate brand or organization. Content of the email may include logos and URLs of the actual organization but feature at least one URL that redirects recipients to deceptive web sites hosting malware that visitors unknowingly download.

The Comodo Threat Research Lab aggressively sets spam traps and honeypots to collect phishing sources, mails and related email senders.

Targeted Phishing

Deceptive websites often masquerade as legitimate brand or organization destinations. Such sites may be hosted on different domains, but the content of the phishing website is designed to mimic that brand or organization, often imitating legitimate login or sign-up pages to deceive visitors.

The Comodo Threat Research Lab analyzes site URLs, content, visual similarities, use of logos and SSL certificate to classify an unknown site as phishing. You can combat phishing attacks by selecting **Phishing** in the Comodo Dome Shield security rules.

PUA Domains – Potentially Unwanted Applications

PUAs are programs with unclear and possibly hidden objectives. A PUA may be executed with the consent of the user but possibly includes behaviors such as bundling, advertising, information collection, etc.

You can block PUAs by selecting **PUA Domains** in Comodo Dome Shield security rules.

Spam and Spammers

Spammers send deceptive or fake emails – spam – to promote scams or fraudulent campaigns to collect private information from companies and end-users. Spam comes in various forms, including distribution of fake banking, social media or business information and soliciations, malware attachments, directory harvesting, etc.

The Comodo Threat Research Lab deploys spam traps and honeypots for active threat hunting and customer protection. You can block access to spam related sources by selecting **Spam Sources** in Comodo Dome Shield security rules.

Spyware

Spyware comprises malicious software that infects customer PCs or mobile devices to collect sensitive and private information. Behavioral sequence analysis run in dynamic analysis environments lets the Comodo Threat Research Lab extract the main characteristics of these threats, including persistence, hidden joint installation with other software, browsing history tracking, capturing keystrokes, collecting authentication details, etc.

You can block spyware by selecting the **Spyware** category in Comodo Dome Shield security rules.

Drive-by Downloads

Drive-by downloads let attackers place malicious executables in a user's environment when users visit a website, open an e-mail attachment, click a misleading links and other ill-advised activities. Download may occur either with or without user permission or knowledge. Fileless malware and/or unpatched vulnerabilities in code running on user's computer may also facilitate such exploits and allow installation of unwanted software.

You can block drive-by downloads by selecting the **Drive-by Downloads** category in Comodo Dome Shield security rules.

IP Scanning and Brute Force Attacks

Scanners and IP Check services run as web services that crawl ranges of IP address and attempt to exploit vulnerabilities encountered. Through sheer brute force, they attempt to access various web services (e.g., data bases) by checking open ports and supplying pre-defined credential sets.

The Comodo Threat Research Lab deployed has multiple honeypots that pose as vulnerable servers for such attacks to collect information about these type of attackers and their systems. You can block sources of these "malicious intent" scans by selecting the **Brute Forcer/Scanner/IP Check** category in Comodo Dome Shield security rules.

Blackhole / Sinkhole

A sinkhole is a DNS server that resolves domain name requests with false results, allowing an attacker to redirect name resolution to potentially malicious destinations. One scenario involving a DNS sinkhole was the infamous CryptoLocker malware. CryptoLocker is ransomware that encrypts user's and then sends the decryption key to a C&C server. Normally a C&C server with a fixed IP or registered domain name would soon be detected and shut down by authorities. To avoid detection, the CryptoLocker C&C server uses random-looking domain names, cycling through them at a high rate. The domain names are generated with a pseudo-random algorithm shared by the malware and C&C server. When CryptoLocker executes on a target computer, it connects the C&C server using one of the randomized domains.

Replaying CryptoLocker-type malware behavior in an isolated honeypot can reveal the sinkhole DNS that the malware uses. You can block blackhole and sinkhole threats by selecting **Blackhole/Sinkhole Systems** in Comodo Dome Shield security rules.

Known DDoS Source:

Distributed denial-of-service attacks (DDoS) are cyber-attacks in which the perpetrator makes a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting operation of the host for that service, usually by flooding it with legitimate service requests. The Comodo Threat Research Lab uses honeypots to attract traffic from malicious DDoS servers and botnets. Aggregating and analyzing the network logs in search network patterns, traffic spikes in logs, repeating offending IP blocks, corelating attacks with specific countries, identifying protocols in use, etc. on a honeypots can reveal possible DDoS servers.

You can block sources of previously recorded DDoS attacks by selecting **Known DDoS Sources** in Comodo Dome Shield security rules.

Fake AV

Fake AV (fake anti-virus) malware infects systems via downloads from malicious websites, spam emails, , deceptive social networking sites and advertisement, or are downloaded by other malware. Fake AV tools promise to clean user systems and remove all malicious software but are actually just malware in disguise.

You can block **Fake AV** sources by selecting Fake AV in Comodo Dome Shield security rules.

Tor Nodes

Tor is a distributed browser and addressing system that helps users protect their identity and anonymity while using the Internet. Tor employs multiple exit relays for connecting to services on these nodes, located in various parts of the world. Some Tor nodes are open to all visitors while others are hidden, findable and reachable only by analyzing Tor network data.

You can block access to TOR network nodes by selecting **TOR Nodes** in Comodo Dome Shield security rules.

P2P Nodes

In traditional client/server configurations, a PC or other device acts as a client and sends requests to a server, a computer on the web or in the cloud, to obtain data or services: browsing the web, fetching email, or streaming content. In a P2P (Peer-to-Peer) paradigm, clients may connect directly to other clients or to multiple peers on a network to share data and services. Unfortunately, P2P nodes on the internet are often employed for malicious purposes by malware publishers and hackers.

The Comodo Threat Research Lab exposes malicious P2P Nodes by analyzing network communication in search of known or Zero-Day malware samples making use of P2P protocols. You can block access to this category of threat by selecting **P2P Sources** in Comodo Dome Shield security rules.

Self-Signed SSL Sites

Comodo Cybersecurity built its original business success as a supply of SSL certificates and remains the leader in generating certificates used to encrypt and secure web traffic. However, some potentially malicious site do not obtain certificates from a Certificate Authority, instead creating their own SSL certificates for their domains and HTTPS traffic. Such domains are frequently employed in fraud-related activities by cyber-criminals to obtain the trust of visitors to that site. Moreover, If the target system is using a browser or OS with vulnerabilities, communications with such sites can provide opening for malware and hackers.

You can block access to sites using self-signed certificates by selecting the **Self Signed SSL Sites** category in Comodo Dome Shield security rules.

VPN Servers

To comply with corporate web security policies, many companies require that employees use client-to-site VPN services to reach company intranets and other sources of critical data and services. But employees and other also use VPN software to end-run web filtering software and other security measures while working behind corporate firewalls. Such attempts not only violate the security policies but also create risks for malicious actors using the same VPN to gain access to the company network via the client machine, via malicious websites or applications that use similar VPN Gateways.

You can block access to VPN services by selecting the **VPN Servers** category in Comodo Dome Shield security Rules.

Mobile Threats

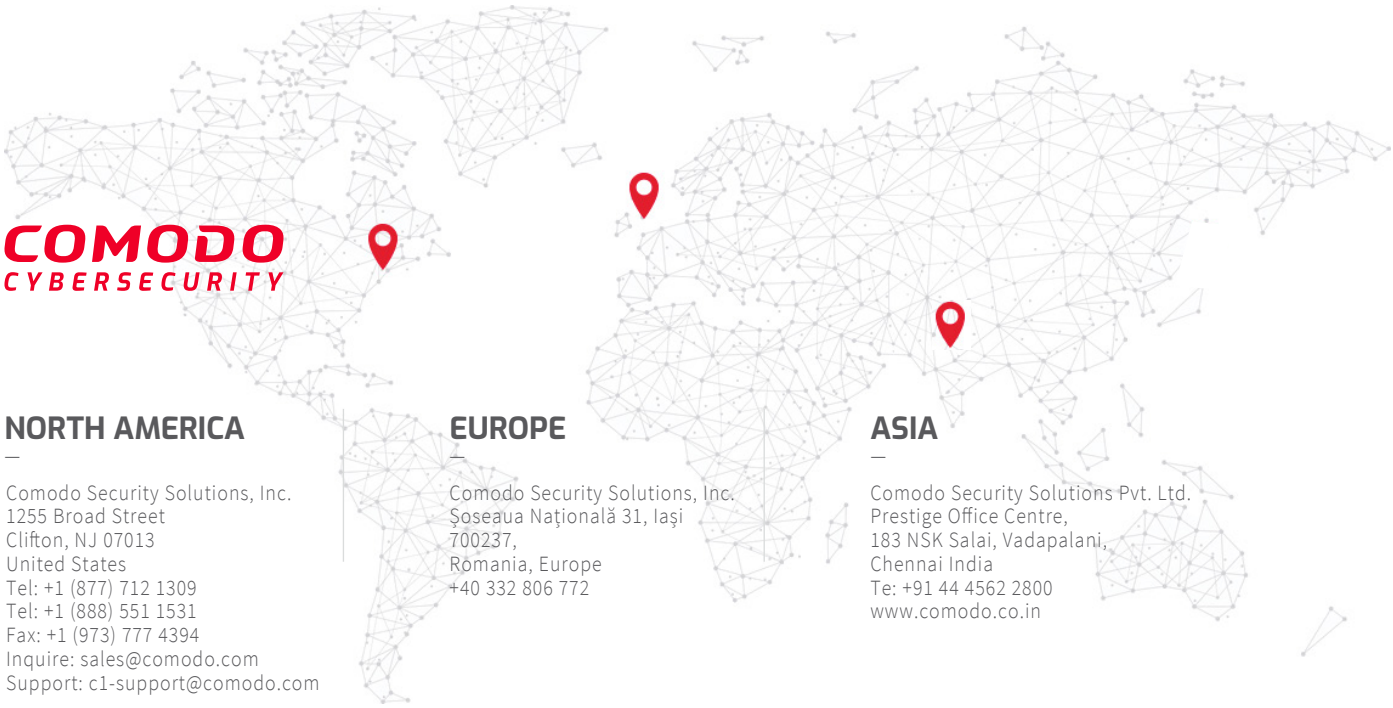
Mobile-specific attacks include injected scripts using responsive property of web sites, spam and phishing, SMS messages using URL shorten services, and malicious Android apps that collect private data from mobile phones.

The Comodo Threat Research Lab analyzes malicious files found on Comodo-protected mobile devices to gather intel on such systems. You can block access to mobile threat sources by selecting **Mobile Threats** in Comodo Dome Shield security rules.

Bitcoin Related Threats

Website owners with malicious intent place hidden Coinhive scripts in their sites to use visitor CPU cycles to mine cryptocurrency. Such parasitic activities lead to excessive usage of user CPU and performance issues. More advanced attackers leverage malware to piggy mining operations on user machines.

The Comodo Threat Research Lab analyzes billions of websites and crypto-mining malware daily to blacklist purveyors of crypto-mining malware. You can block access to Coinhive and cryptocurrency miners by selecting the **Bitcoin Related** category in Comodo Dome Shield security rules.



COMODO
CYBERSECURITY

NORTH AMERICA

Comodo Security Solutions, Inc.
1255 Broad Street
Clifton, NJ 07013
United States
Tel: +1 (877) 712 1309
Tel: +1 (888) 551 1531
Fax: +1 (973) 777 4394
Inquire: sales@comodo.com
Support: c1-support@comodo.com

EUROPE

Comodo Security Solutions, Inc.
Şoseaua Națională 31, Iași
700237,
Romania, Europe
+40 332 806 772

ASIA

Comodo Security Solutions Pvt. Ltd.
Prestige Office Centre,
183 NSK Salai, Vadapalani,
Chennai India
Te: +91 44 4562 2800
www.comodo.co.in

VISIT COMODO.COM

REQUEST A DEMO

Try Comodo Cybersecurity by speaking with a security consultant to begin the process to set up a demo or proof-of-concept project. Contact us directly at +1 888-266-6361

Stay in the loop