


HAT Report: Hidden Abuse and Threats in Your Network

The HAT Report is designed to provide an easy to view snapshot of Abuse and Threats hidden within your network.

The Report is based on the CIDR blocks provided and gives you an up to date view of abuses and threats on your resources within your network.

Actual existing abuse, by category, is presented for use by your security and abuse mitigation teams.

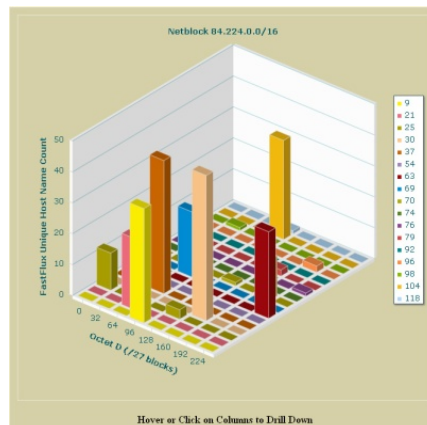


Netblock	FastFlux	Malware	Phishing	Snowshoe/Spam	Listed Domains	rDNS	BotNet	Name Servers	C&C
64.236.0/16	FastFlux: 1	malware: 9	phishing: 2	clean	clean	*	XBL: 2	malware: 45	*
64.236.34.0/16	clean	clean	clean	clean	clean	*	XBL: 4	malware: 12	*
64.236.0/17	clean	malware: 1	phishing: 13	SBL78139	clean	*	XBL: 3	malware: 1872	*
64.236.0/18	clean	malware: 22	phishing: 48	clean	clean	*	XBL: 3	malware: 50	*
64.236.0.0/16	clean	malware: 11	phishing: 15	clean	clean	*	XBL: 13	malware: 24	*
64.236.32.0/16	FastFlux: 16	malware: 150	phishing: 173	clean	clean	*	clean	malware: 11	*

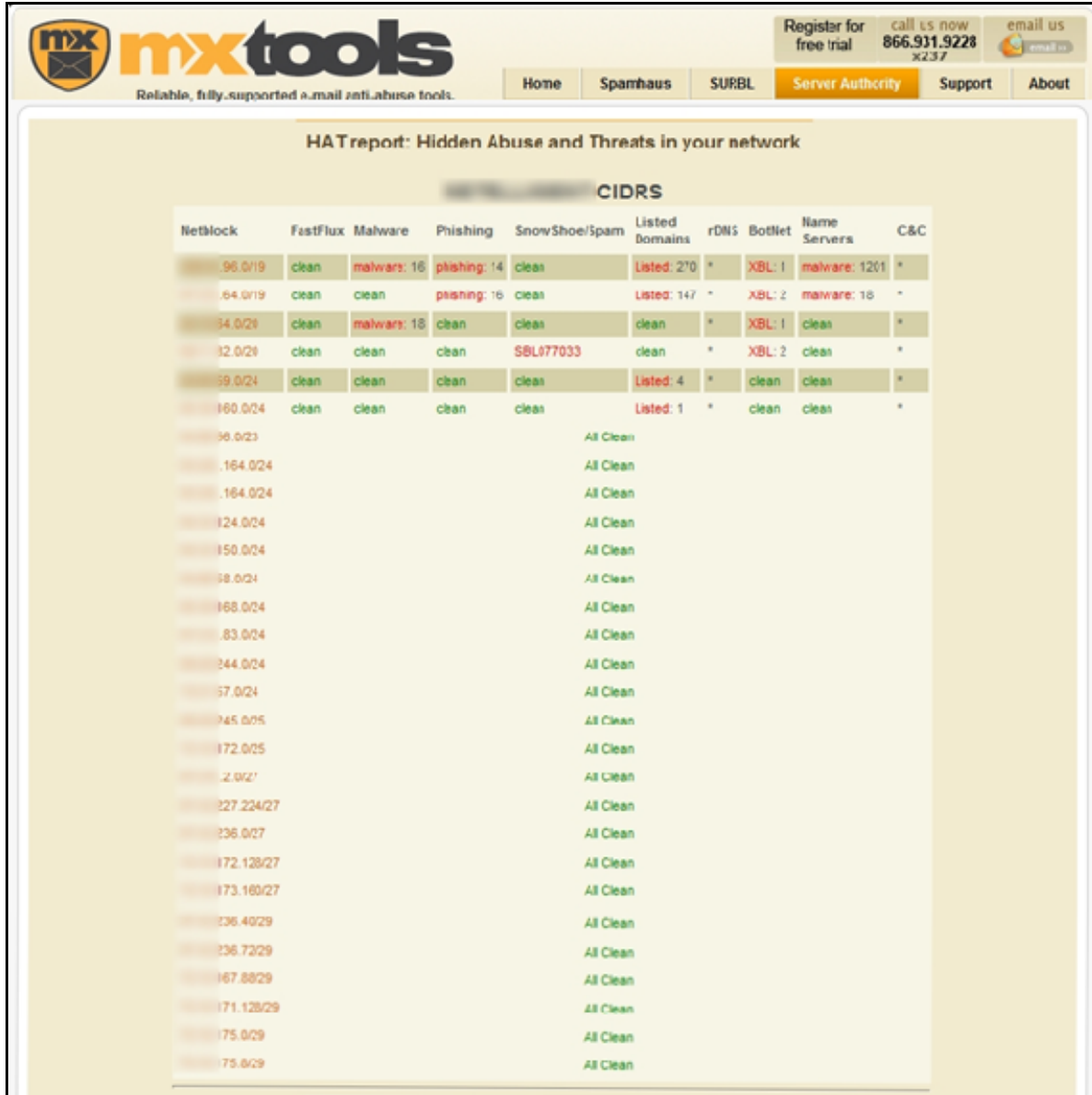
Quickly and easily identify the following Abuses and Threats within your Network:

- FastFlux
- Malware
- Phishing
- SnowShoe Spam
- SURBL listed domains
- BotNet
- Nameservers delivering malware
- Command and Control center

And find where they're hiding...



Example HAT report



HAT report: Hidden Abuse and Threats in your network

CIDRS

Netblock	FastFlux	Malware	Phishing	SnowShoe/Spam	Listed Domains	rDNS	BotIet	Name Servers	C&C
196.0/19	clean	malware: 16	phishing: 14	clean	Listed: 270	*	XBL: 1	malware: 1201	*
164.0/19	clean	clean	phishing: 16	clean	Listed: 147	*	XBL: 2	malware: 16	*
134.0/21	clean	malware: 18	clean	clean	clean	*	XBL: 1	clean	*
132.0/21	clean	clean	clean	SBL077033	clean	*	XBL: 2	clean	*
139.0/24	clean	clean	clean	clean	Listed: 4	*	clean	clean	*
160.0/24	clean	clean	clean	clean	Listed: 1	*	clean	clean	*
196.0/23					All Clean				
164.0/24					All Clean				
164.0/24					All Clean				
124.0/24					All Clean				
150.0/24					All Clean				
148.0/24					All Clean				
168.0/24					All Clean				
83.0/24					All Clean				
244.0/24					All Clean				
157.0/24					All Clean				
145.0/25					All Clean				
172.0/25					All Clean				
172.0/27					All Clean				
172.128/27					All Clean				
173.160/27					All Clean				
136.40/29					All Clean				
136.72/29					All Clean				
167.88/29					All Clean				
171.128/29					All Clean				
175.0/29					All Clean				
175.0/29					All Clean				

Get a free HAT report for your network!

Contact MXTools:

1.866.931.9228 x237

International Phone: +1.778.330.1074 x237

support@mxttools.com



HAT Report: explanations and suggested actions:

FastFlux

FastFlux hosts within your network are hosts that have been compromised and are under miscreant control. The miscreant in this case is likely not one of your customers. FastFlux is a technique for providing a type of "bullet-proof" hosting for criminal activities. The FastFlux network provides an endless supply of IPs sprayed across many ASNs and countries, usually on high bandwidth connections such as home or office users who are infected with a virus. Since the web, email or DNS servers proxied through these hosts can go down and just be replaced automatically by the next compromised host in the miscreant's database.

More detail: Click on the word FastFlux in the HAT report to see more detail of malicious hostnames that have been resolving into your IP space on specific IPs. ZoneCruncher users have access to the most detail; for a ZoneCruncher trial please contact Arnie Bjorklund arnieb@mxtools.com.

Recommended action: Observe active ports on listed hosts to verify that the IP is still assigned to a compromised machine. Place the machine into a walled garden or disconnect connectivity until the machine can be cleaned of infection and secured. <http://Secure411.org> provides free info on disinfecting and securing Windows machines. Note that the best way to disinfect is to boot to a clean non-windows operating system such as the free TRK Trinity Rescue Kit which is designed specifically for the purpose of providing multiple anti-malware / anti-virus scans.

Malware

Malware is usually an executable file that is being delivered or redirected through one of your IPs. The machine involved may have had malicious executables intentionally placed there by one of your customers who is intentionally enticing innocent victim's computers to download and install the malware. Or your customer's site may have been hacked by an outsider who managed to upload a file to a location such as a web or FTP server. Or your IP may be in use in one or more redirections such that the actual malware to be downloaded is not on your machines but your machines are being used to redirect traffic to the malicious download site.

More detail: Click on the word Phishing in the HAT report to see more detail for a list of domains and IPs involved in the malware incident. Sometimes you may also be able to get the full URL where the executable file was spotted. A Google search may bring up info related to the malware incident.

Recommended action: Search the www folders on the affected machine for executable files. Move those found to be malware and all executables without a known necessary purpose. Save an archive of all files related to the potential malware. Preserve log files and customer records that could lead law enforcement to the miscreants responsible. Change FTP and other user/passwords that may have been



used to give the criminal access. Determine exploits used such as PHP or script vulnerabilities and install patches or put restrictions in place to prevent repeat infections. Stop providing service to customers complicit with the miscreant and find any related resources that same customer is obtaining from you.

Phishing

A phish is usually a website that is an illegal copy of a well-known financial or restricted access page. Miscreants use these fake pages to collect victim's users, passwords, or other personal or financial secrets that would allow miscreants to access funds or sell private information. The domain the phishing site is hosted on could belong to a malicious customer - such as pay-pals.com. In other cases, you have a legitimate customer with an insecure compromised web server, so the phishing site will appear such as <http://joeshardware.com/.wachovia/>.

More detail: Click on the word Phishing to see any available detail. After viewing the domain associated with the phishing incident, try a Google search for any public information or URLs available on phishing report sites.

Recommended action: Remove all phishing files from the machines under your direct control by using a "whole system" file search for the offending file names. Save an archive of all files related to the hacking / phishing. Preserve log files that could lead law enforcement to the miscreants responsible. Change FTP and other user/passwords that may have been used to give the criminal access. Determine exploits used such as PHP or script vulnerabilities and install patches or put restrictions in place to prevent repeat infections.

Snowshoe / Spam

Snowshoe is a spammer technique where spam is emitted from many different IPs in a netblock. IPs are discarded as they are blacklisted for spamming. Usually you can see rDNS with a distinct pattern of numerically incremented hosts or similar naming convention domains. The rDNS may have subdomains with "mx" in the hostname. The base domain will usually match the domain that will be used in the envelope-from of the spam run. Domains, hosts and the emitter IP are "throw-away" - cease to be used after they appear on popular blacklists.

More detail: Click on the SBL link for publically available detail on the incident. ZoneCruncher users may have access to additional details; for a ZoneCruncher trial pass please contact Arnie Bjorklund arnieb@mxtools.com.

Recommended action: Cut off connectivity to the customer involved in the spam / snowshoe operation. Clean the rDNS in the affected ranges to nothing or your generic rDNS. Find all resources you are providing to related customer accounts and cut off connectivity to any that are set up for malicious activity.



Listed Domains

Listed domains are on a blacklist for general reasons such as non-whitelisted domains appearing in URLs that are hitting spamtraps.

More detail: Click on the link for a list of the domains that resolve to your IPs. A Google search, visit to the domain website, or whois look up may yield more detail.

Recommended action: Check the websites and other resources you are providing that support operations with these domains and look for signs of selling spam-vertised products or other undesirable activities. Terminate customers in violation of your AUP and seek out all related resources you are providing to same customer accounts / names / credit cards etc.

rDNS

The rDNS column hits represent any suspicious domains found in the reverse DNS host for the IPs in the specified netblock.

More detail: Click on the link to see a list of the suspicious reverse DNS host names.

Recommended action: Check who requested the rDNS hostnames and evaluate that customer for termination based on your AUP if you find current malicious behavior. Clean up rDNS to blank or your generic rDNS if the customer is gone.

BotNet

The BotNet column represents compromised hosts that are usually part of a spam emitting large scale controlled network.

More detail: Click on the XBL link to see a list of your affected IP addresses.

Recommended action: Observe active ports on listed hosts to verify that the IP is still assigned to a compromised machine. Place the machine into a walled garden or disconnect connectivity until the machine can be cleaned of infection and secured. <http://Secure411.org> provides free info on disinfecting and securing Windows machines. Note that the best way to disinfect is to boot to a clean non-windows operating system such as the free TRK Trinity Rescue Kit which is designed specifically for the purpose of providing multiple anti-malware / anti-virus scans.

Name Servers

These are name servers located within your network which are supporting malicious activities such as domains used in spam, for malware distribution, phishing or other malicious activities.

More detail: Click on the link for a list of the name servers on your IPs and a list of the offending domains they serve.



Recommended action: Cut off service to your customers who are violating your AUP by providing DNS resources supporting malicious activities. Find all related activities of the same customer account or related accounts

C & C

C & C is the abbreviation for Command and Control, usually IPs in your network that are in use by botmasters as control points for their network of compromised hosts.

More detail: Click on the link for a list of your involved IPs.

Recommended action: Save an archive of all files related to the command and control host. Preserve log files and customer records that could lead law enforcement to the miscreants controlling the botnet. Change FTP and other user/passwords that may have been used to give the criminal access. Determine exploits used such as PHP or script vulnerabilities and install patches or put restrictions in place to prevent repeat infections. Stop providing service to customers complicit with the miscreant and find any related resources that same customer is obtaining from you.