Digital Brand Protection

MALWARE

Detection and Prevention

Fully Managed Threat Hunting, Intelligence, Detection and Takedown of Threats to your brand outside your perimeter online.

Fully Managed Threat Hunting, Intelligence, Detection and Takedown of Threats to your brand outside your perimeter online.

Malware (Banking Trojans / Crimeware) Detection and Takedown

Analysis and unpacking of malware in the wild to detect and takedown crimeware developed to specifically target your organisation and your customers.

Through a combined process of automated and human analysis, FraudWatch focusses on identifying all components of malware, from the drop sites and command and control servers. We provide a fully managed service, detecting, assessing, and analysing potential threats through to the take down of malware components by our Human Analysts in our 24 X 7 Security Operations Centre (SOC).

Banking Trojan Malware silently infects end users on both mobile and desktop devices stealing account credentials unnoticed or silently hacking secure sessions.

Proactive malware detection

At its core malware is code or software that’s injected into a web-system in order to cause damage. Intentions and capabilities range from taking control of computer systems and corrupting software to stealing information. Malware comes in many different forms – from viruses and spyware to ransomware and trojans – all targeting your organisation and your customers. With so many things to look out for, malware can be easy to miss. By teaming up with FraudWatch you will gain a team of dedicated malware analysts that source malware circulating in the wild through network relationships and data feeds. This malware is then unpacked and analysed to determine if it is targeting your organisation. If it is – further analysis is then performed to identify the command-and-control servers (C&C) and Credential drop sites. All the while giving you the confidence that your website is protected.

Malware protection and prevention

FraudWatch uses expert human analysts in our 24×7 Security Operation Centre (SOC) to spearhead the malware component takedown process. We do much more than simply send an automated single email to an abuse mailbox. Our team analyses each hosted component to determine all possible parties involved and work tirelessly to contact them. As a result of our extensive experience in the industry, in many cases, we have a direct reporting process for immediate takedown of malicious software.

Once all back-end infrastructure of the malware is taken down, it is rendered inoperable, regardless of the number of devices infected. The malware simply cannot communicate and provide stolen data or credentials back to the criminals. Working in conjunction with our exceptional DMARC and Phishing solutions will ensure overall protection of your company's assets.

Malware solutions are our business – which gives you the confidence to focus on your own.

Proactive malware detection

At its core malware is code or software that's injected into a web-system in order to cause damage. Intentions and capabilities range from taking control of computer systems and corrupting software to stealing information. Malware comes in many different forms – from viruses and spyware to ransomware and trojans – all targeting your organisation and your customers. With so many things to look out for, malware can be easy to miss. By teaming up with FraudWatch you will gain a team of dedicated malware analysts that source malware circulating in the wild through network relationships and data feeds. This malware is then unpacked and analysed to determine if it is targeting your organisation. If it is – further analysis is then performed to identify the command-and-control servers (C&C) and Credential drop sites. All the while giving you the confidence that your website is protected.

Malware protection and prevention

FraudWatch uses expert human analysts in our 24×7 Security Operation Centre (SOC) to spearhead the malware component takedown process. We do much more than simply send an automated single email to an abuse mailbox. Our team analyses each hosted component to determine all possible parties involved and work tirelessly to contact them. As a result of our extensive experience in the industry, in many cases, we have a direct reporting process for immediate takedown of malicious software.

Once all back-end infrastructure of the malware is taken down, it is rendered inoperable, regardless of the number of devices infected. The malware simply cannot communicate and provide stolen data or credentials back to the criminals. Working in conjunction with our exceptional DMARC and Phishing solutions will ensure overall protection of your company's assets.

Malware solutions are our business – which gives you the confidence to focus on your own.

Contact Us to discuss current Malware Threats targeting your brand.

Contact us for a Scan of current Malware Threats targeting your brand.