PHISHLABS

Crimeware Protection

Detect, stop, and prevent crimeware attacks around-the-clock.

Used by cybercriminals to take over online accounts used for banking, shopping, gaming and other transactions, crimeware enables the theft of billions of dollars every year. Today's crimeware is professionally developed and sold in thriving underground markets, giving even novice cybercriminals the ability to attack businesses and their customers, harvest user credentials, hijack accounts, and carry out fraud.

Because crimeware attacks commonly use banking Trojan kits that are designed for stealth, such as ZeuS, Dyre, and Vawtrak, it is difficult for institutions to detect crimeware attacks against their customers. And while strong authentication and fraud prevention controls make it harder for cybercriminals to carry out fraudulent transactions using stolen credentials, cybercriminals are quick to develop new malware functionality that evades anti-fraud mechanisms.

Protect against crimeware attacks used to take over accounts

PhishLabs takes a different strategy to protect against crimeware attacks. We aggressively fight back against the cybercriminals that use banking Trojans and other malware to steal credentials, take over accounts and carry out online fraud. We detect, analyze and proactively dismantle the systems and illicit services used to carry out crimeware attacks. Our approach disrupts the cybercrime ecosystem, impeding profits and requiring cybercriminals to rebuild before launching new crimeware attacks.

Service features

24/7/365 crimeware attack detection and mitigation

Shut down of all malicious URLs, domains and other attack points

Actionable intelligence on malware used in the attack

Disruption of the underlying cybercrime ecosystem

Fixed fee, unmetered service pricing

When malware targeting your account holders is detected, we quickly shut down the sites hosting the malware to prevent additional infections. But we do not stop there. We dive far beneath the surface of the attack to disrupt the cybercrime ecosystem that is used to plan, stage, launch and monetize crimeware attacks.

> *"We're hearing that the fraud has evolved, there are new types of malware being deployed and, particularly in those banks that have yet to put in robust solutions, we're seeing that fraud spike again," says Shirley Inscoe, senior analyst with Aite Group[1].*

+1.877.227.0790 info@phishlabs.com

Rapid detection and shut down

New crimeware attacks are detected by proprietary automated malware analysis systems and the PhishLabs Threat Research Team. Global malware data is fed into our automated systems from a broad network of public and private sources including:

- Anti-virus partners
- Email provider spam data
- Security community relationships
- VirusTotal
- Spam pots
- Client reports

The PhishLabs Threat Research Team provides even greater crimeware visibility and intelligence. This team investigates the underground cybercrime ecosystem, hunting crimeware and developing intelligence that cannot be sourced via automated feeds and relationships.

Malware data from feeds and the PhishLab Threat Research Team is analyzed to detect crimeware targeting our clients and their customers. When an attack is detected, key shut down data is automatically and manually extracted including the URLs of the malware executable, configuration files, update files and data drops. This data is automatically packaged and sent to the 24x7x365 Security Operations Center which rapidly shuts down the points of attack.

Prevent victimization and future attacks

PhishLabs experts go beyond shutting down the web pages serving the crimeware executable. We fight back against the cybercrime ecosystem by:

- Shutting down config and update URLs
- Shutting down malware and exploit kits
- Broadcasting malware URLs and binaries to security partners
- Recovering stolen credentials
- Investigating cash out operations
- Conducting ongoing reconnaissance
- Supporting law enforcement action

Our approach disrupts the cybercrime ecosystem, impeding profits and requiring cybercriminals to rebuild before launching new crimeware attacks. Cybercriminals then move on to softer targets that do not fight back.

About PhishLabs

PhishLabs is the leading provider of 24/7 cybersecurity services that protect against the exploitation of people to compromise systems and steal data. PhishLabs combines proprietary technology, intelligence, and human expertise to rapidly detect, analyze, and stop targeted cyberattacks before they impact organizations.

To learn more, visit www.phishlabs.com.

+1.877.227.0790 info@phishlabs.com

1 http://www.americanbanker.com/issues/178_194/wire-and-online-banking-fraud-continues-to-spike-for-businesses-1062666-1.html