LOOKINGGLASS

MALWARE TOTAL LIFECYCLE PROTECTION

Real-Time Awareness of Malicious C2, Phishing and Malicious URLs

The LookingGlass Malware Total Lifecycle Protection (TLP) data feed bundle offers real-time awareness of command and control (C2) domains, phishing URLs, and malicious URLs for immediate action by your security operations and infrastructure. The bundle consists of three LookingGlass threat intelligence data feeds:

- Malicious C2 Feed
- Phishing URL Feed
- Malicious URL Feed

Together, these feeds provide up-to-the-minute awareness of malicious activity "in the wild" – before it reaches your network perimeter.

Organizations utilizing LookingGlass Phishing Solutions can include the LookingGlass Protected Site Seal on their website. The seal is a known trust mark that indicates your company provides early detection and immediate mitigation of sites used for phishing attacks, as well as proactively protects customers from online fraud and identity theft.

LOOKINGGLASS MALWARE TOTAL LIFECYCLE PROTECTION TLP SPECIFICATIONS

Threat Intelligence Feed Name	Formats Available
LookingGlass Malicious C2 Feed	OpenTPX CSV File
LookingGlass Phishing URL Feed	Secure XML
LookingGlass Malicious URL Feed	Secure XML Secure FTP

Comprehensive Threat Intelligence Feeds

Malicious C2
Delivers a daily updated list of fully qualified domain names (FQDNs) associated with infected C2. The list of malicious domain names is generated from a combination of LookingGlass virus and botnet tracking, sinkhole servers, and reverse engineering of domain-generation algorithms (DGA) and analysis of advanced persistent threats (APTs).

Phishing URL Feed
Delivers a near real-time stream of URLs that host phishing attacks. The feed is gathered from a variety of sources including spam email, domain name registrations, proprietary web crawling technology, "suspect email" streams from major web-based email providers, and patented LookingGlass Site Seal technology. It is then quality controlled by experienced multilingual threat analysts.

Malicious URL
Delivers a near real-time stream of URLs that attempt to infect user computers with malicious code when the user accesses the URL. Discovered malicious URLs are gathered from a variety of sources, including spammed links, suspicious domain name registrations, phishing attacks, "suspect email" streams from major web-based email providers, and patented LookingGlass Site Seal technology. It is then analyzed and tested against multiple antivirus engines and security programs by the LookingGlass Malware Lab.

FEATURES	BENEFITS
Pre-Infection Protection	• Detect threats before they enter your network perimeter. • Protect your organization from users or malware accessing potentially harmful web links.
Post-Infection Protection	• Limit and block outgoing traffic from infected machines from reaching C2 servers.
Broad Security Coverage	• Import feed data into your existing network security appliances.
Open TPX	• Modular, comprehensive open schema for sharing Internet and threat intelligence, as well as providing for efficient transfer data. It is based on years of experience building scalable threat intelligence and security products that exchange data at large volumes and high speed. • Conveys all aspects of the threat data in its most basic element with minimal interpretation at data ingest to enable efficient information processing. • Simplifies the task of visualizing and correlation the multiple diverse forms of threat intelligence.
Ease of Implementation	• Ingest feeds in less than a day. • Available using open transports with open formats.

ABOUT LOOKINGGLASS CYBER SOLUTIONS

LookingGlass Cyber Solutions delivers unified threat protection against sophisticated cyber attacks to global enterprises and government agencies by operationalizing threat intelligence across its end-to-end portfolio. Scalable threat intelligence platforms and network-based threat response products consume our machine-readable data feeds to provide comprehensive threat-driven security. Augmenting the solutions portfolio is a worldwide team of security analysts who continuously enrich our data feeds and provide customers unprecedented understanding and response capability into cyber, physical and 3rd party risks. Prioritized, relevant and timely insights enable customers to take action on threat intelligence across the different stages of the attack life cycle. Learn more at **https://www.lookingglasscyber.com/.**

Know More. Risk Less.

TechDefcon

TechDefcon
Dubai, United Arab Emirates 242727
+971504529715 / +97143596595
www.techdefcon.com / info@techdefcon.com