ThreatSTOP

ThreatSTOP presents

7 OPEN SOURCE ANALYSIS TOOLS, TIPS & USE CASES

#1: USE IOCs TO PROACTIVELY BLOCK KNOWN THREATS

Before opting for complex and expensive behavior-based security solutions to ensure network and device safety, there is a question that needs to be asked: *Have we ensured that already-known threats are being blocked?*

There are millions of public, free IOCs circling the web, yet the fact that they are openly published does not necessarily mean that they are being utilized for the protection that they can provide. Many times, security solution seekers tend to jump a few steps ahead to very complex technological solutions, while missing out on a huge portion of the threat landscape that should be blocked – known, published threats. IOCs such as IPs and Domain Names can be used to block malicious inbound and outbound traffic, preventing attacks and breaches.

Collect published indicators, analyze them and integrate them in to your security solution to block dangerous known threats, or choose a solution that automates the process, using IOCs and threat intelligence feeds to block these known threats from your system.

#2: THREAT EXCHANGES & IOC SHARING

The first step in IOC analysis is obtaining the indicators to analyze. Some analysts will opt to stick with one source and analyze whichever IOCs come their way. Others may search various sources for a specific threat type, such as Ransomware, or a threat like Lokibot. Threat exchanges are open and free community platforms for information sharing and collaboration, and are an excellent source for IOCs. Another source for IOC collection which may come off as less intuitive is social media, with Twitter being the best SM platform to find new, relevant IOCs.

Our Top 5 Free IOC Sources for Analysis:

1. OTX (Open Threat Exchange)
2. ThreatConnect Exchange
3. MISP (Malware Information Sharing Platform)
4. IBM X-Force Exchange
5. Twitter

Read more **here**

#3: ANALYZING THREAT INFRASTRUCTURE

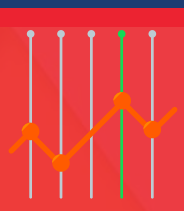
Analyzable indicators can be found on a variety of platforms and channels, each with its own level of reliability and information detail. Once an analyst has deemed the collected IOCs suspicious, they can review its background and infrastructure information, such as ASN and passive DNS for IPs, and Whois, resolving IPs, and popularity score for domains. In addition, the analyst can also check if leading security vendors have already deemed the IOC malicious by choosing from a wide array of open-source blacklists. At the end of this process, the analyst will have the information and knowledge required to decide if the inbound and/or outbound traffic to the indicator should be blocked.
Don't have an analysis team? You'll need to find a reliable vendor that performs this type of analysis to ensure high accuracy and low false-positives in the IOCs you're blocking.

5 free, open-source tools to collect technical and reputation information on IPs and domains:

1. VirusTotal
2. Threat Intelligence Platform
3. IPVoid & URLVoid
4. DNSdumpster
5. CIRCL BGP Ranking

Read more **here**

#4: ENRICHMENTS & CONNECTING THE DOTS



Making connections and finding new indicators is an important part of IOC analysis, and is probably the most enjoyable part as well. Blog posts and reports on new threats will usually mention the indicators seen to be used by the specific malware sample or attack vector analyzed, yet in many cases there is a larger malicious infrastructure behind them just waiting to be uncovered (and blocked!). Sometimes, a whole other malicious infrastructure can be revealed by examining IOCs related to malicious IPs and domains. There are a variety of tools out there that can help analysts investigate indicators of compromise and their infrastructure, and perform enrichment to shed light on related, malicious IOCs.

Below are the ThreatSTOP Security Research Team's favorite connection and enrichment platforms.

1. ThreatCrowd
2. VirusTotal (again)
3. PassiveTotal
4. Yeti

Read more **here**

#5: EMOTET BANKING TROJAN USE CASE

ThreatSTOP's Security Research Team has come across endless Emotet indicators of compromise, which comes as no surprise considering how widespread the malware's activity is.

In addition to automated ThreatSTOP Emotet IOC feeds, the team reviews Emotet indicators posted on sharing platforms in an in-depth analysis, to ensure reliability and to search for additional malicious indicators, as many Emotet IOCs have been found related to additional malicious activity in the past.

READ USE CASE

#6: GUILDMA INFORMATION STEALER USE CASE

This malware is spread via phishing emails, supposedly sent by the Federal Public Ministry of Brazil, containing malicious links. The link downloads a ZIP file containing another ZIP file, which in turn contains a LNK file that executes a malicious JavaScript. The machine is infected, Guildma accesses Facebook and YouTube profiles created by the cybercriminals that host encrypted lists of its C2 servers.

This new Guildma variant was brought to our Security Research Team's attention via an OTX (Open Threat Exchange) pulse, including a link to a report by ISC. Their in-depth analysis noted that this ongoing campaign has 76 C2 servers (and counting), so our team set out to analyze the IOCs and discover additional C2 servers in the malware's infrastructure.

READ USE CASE

#7: ANALYZING APT 10 USE CASE

In April 2019, activity by the Chinese cyber espionage group APT10 was recognized by enSilo. This new campaign boasted previously undiscovered variants of malware and payloads showing many similarities to APT10's previous campaigns. PlugX, a modular malware spotted in the campaign, is developed by the espionage group themselves and has been widely used in the past for targeted attacks against government and private organizations.

In enSilo's report, 6 out of the 7 domains posted in their Indicators of Compromise section were typosquat domains. The ThreatSTOP Security Team decided to take a closer look at these malicious domains.

In this use case, we show how our analysis team used free open-source analysis tools mentioned in previous posts to analyze APT10 campaign domains.

READ USE CASE

Read the Full Blog Series Here

Visit us at www.threatstop.com

ThreatSTOP is a SaaS solution that automatically blocks malicious IP and DNS connections that stop threats like ransomware, phishing, and botnets from infecting your network.

Follow us @ThreatSTOP