ANOMALI

The State of OSINT

An Anomali Threat Research Briefing

ANOMALI eBook

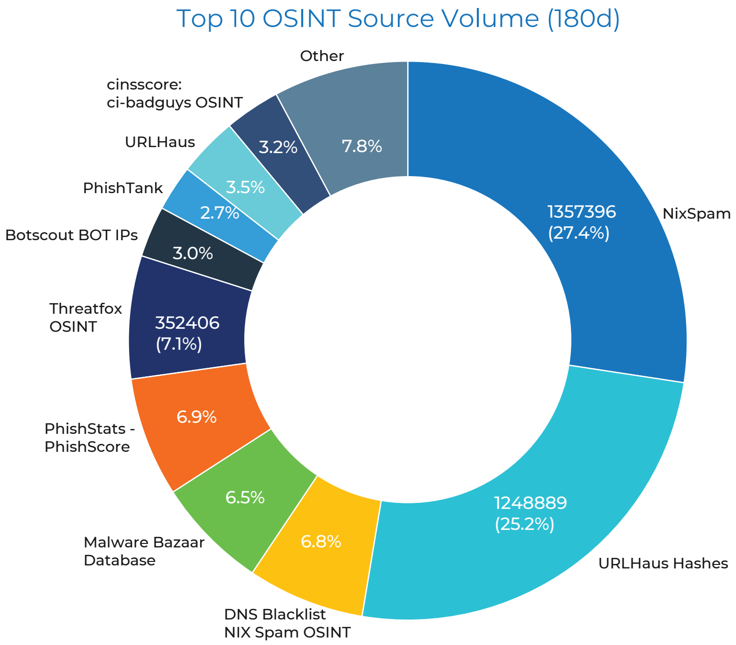
Table of Contents

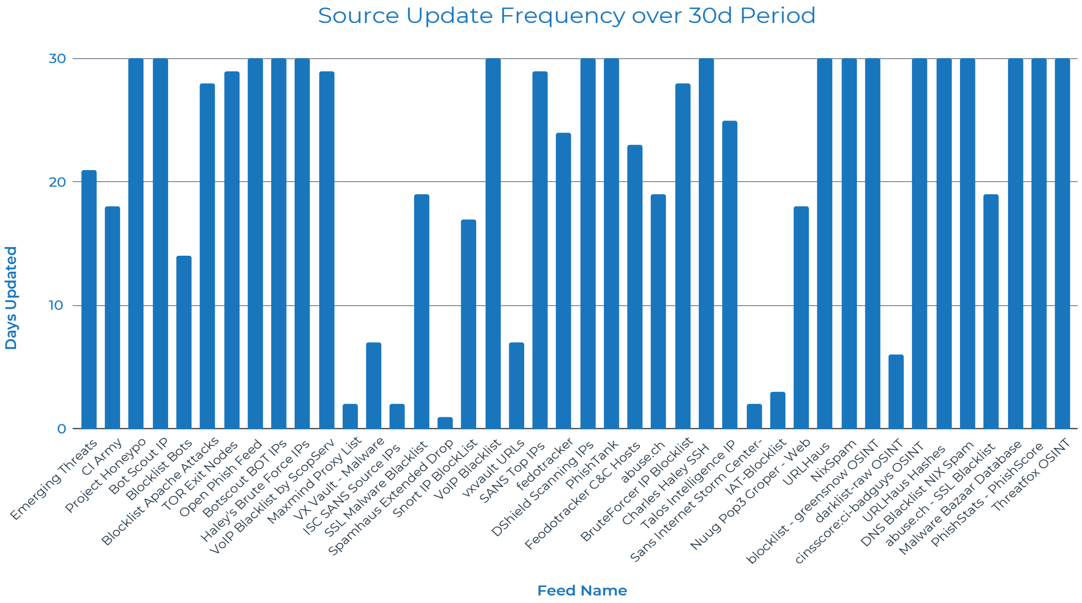
Introduction

Open source intelligence (OSINT) has grown significantly in recent years and become increasingly important in better understanding the cyber threat landscape. Security professionals often use OSINT to help identify network weaknesses and strengthen security solutions. There also exist big challenges with OSINT, such as information overload, uncertainty management and data quality. In this eBook, we provide our study to reflect the current state of OSINT and aim to help alleviate the challenges in dealing with OSINT. More specifically, we focus our analysis on the following aspects: intelligence sources, intelligence collected by Anomali, top 10 malware attribution, and analysis of false positives.

Intelligence Sources

The pie chart below shows the indicator of compromise (IoC) volume distribution of the top 10 most active OSINT sources over 180 days; the bar chart indicates how frequently all examined OSINT sources (44 in total) update over 30 days.





ANOMALI

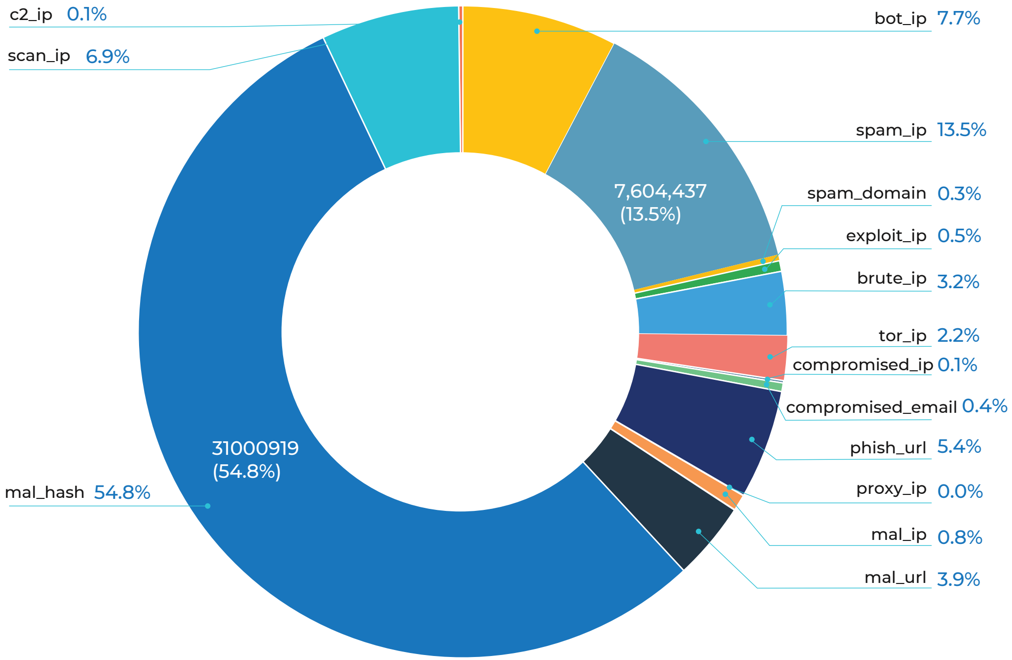
Intelligence Collected

This section shows the IoC volume distribution of various OSINT threat types Anomali collected in 180 days.

As seen from the chart, malware file hash IoCs (more than 31 million) are over 50% of all IoCs collected, followed by spam and bot IP addresses.

Some threat types only have small IoC volumes such as Tor and C2 IP addresses, but they can provide extremely valuable threat hunting intelligence.

OSINT Threat Type Coverage (180d)



ANOMALI

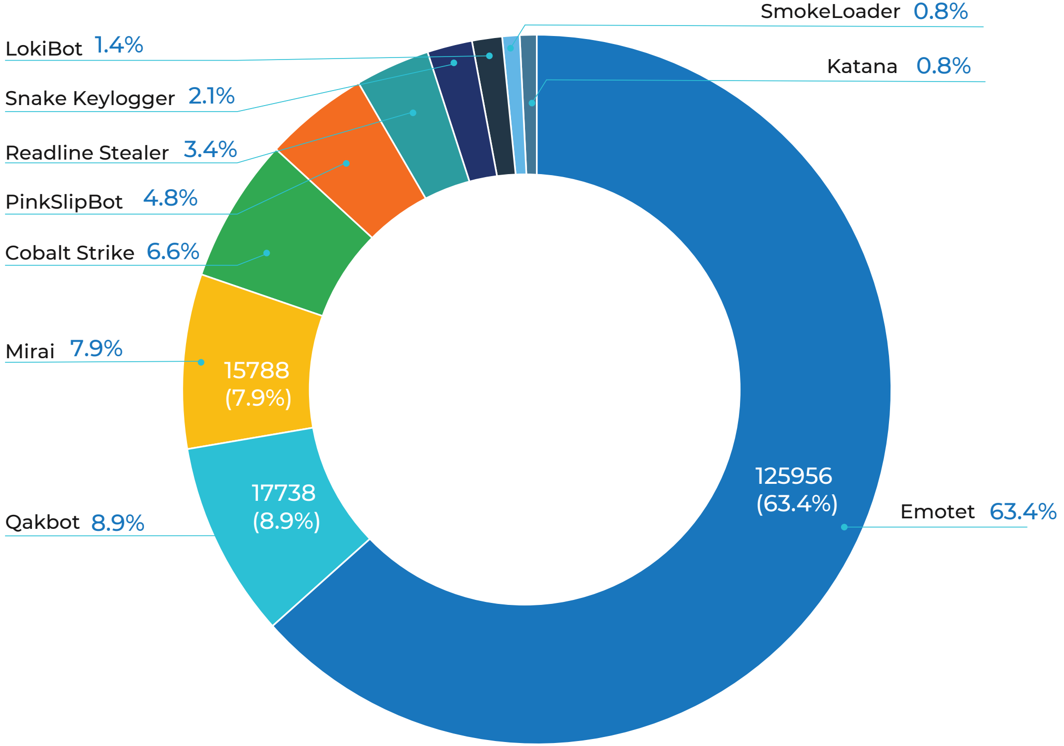
Top 10 Malware Attribution

The chart on the right shows OSINT top 10 malware attribution over 180 days, which is dominated by Emotet.

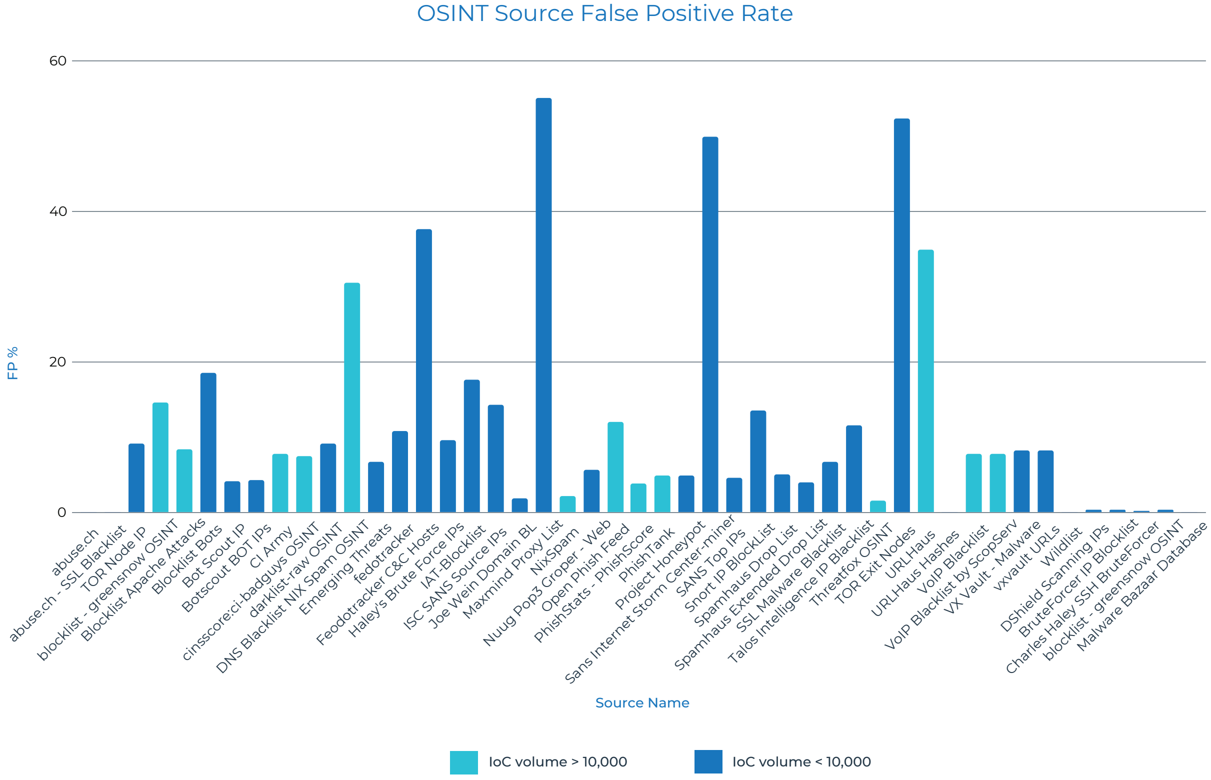
Emotet resurfaced nearly a year after the law enforcement disruption which took place in early 2021, and quickly became the most popular malware in 2022.

Other popular malware includes Qakbot (infostealer) and Mirai (botnet). The last two malware families in the chart are SmokeLoader and Katana, with 0.8% each.

OSINT Top 10 Malware Attribution



Analysis of False Positives



The chart on the left examines the data quality of OSINT sources.

Some sources demonstrate great data quality with low false positive (FP) rates and high volumes, such as NixSpam and Threatfox OSINT.

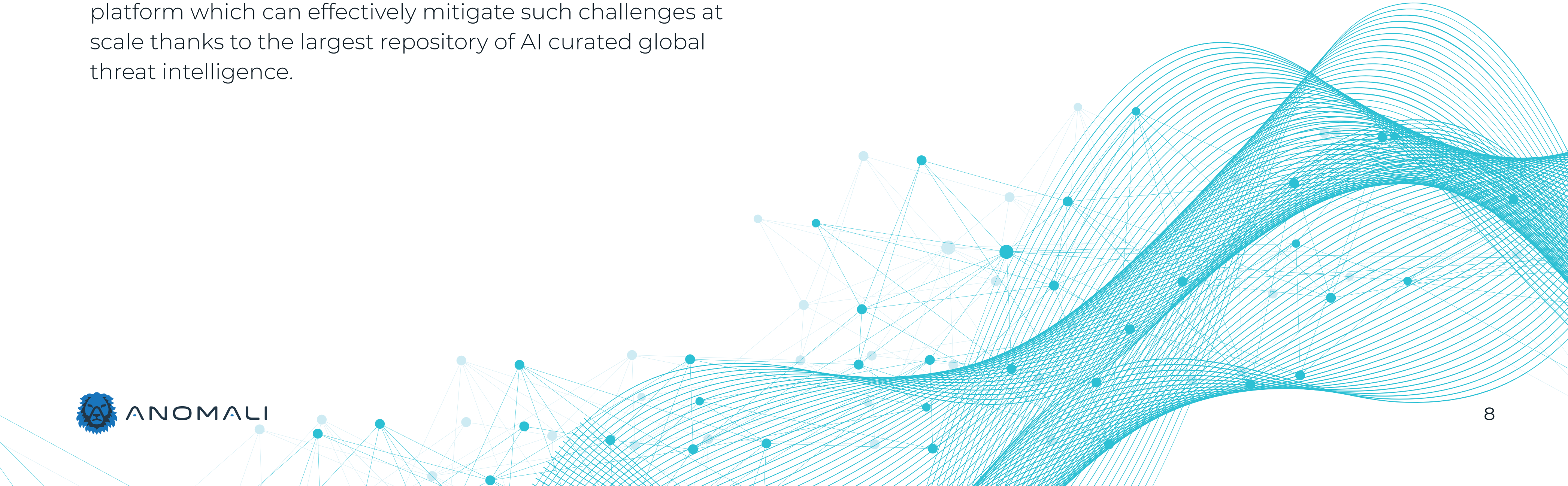
A few OSINT sources with both high and low volumes actually have really high FP rates (over 30%).

Extra care should be taken when dealing with sources exhibiting high FP rates, especially those with high volumes. Data with low signal-to-noise ratio (SNR) can complicate analysis and mislead results.

Conclusion

Undoubtedly, OSINT data provides great value in helping threat hunting and detection. The state of OSINT from our research provides some interesting findings to help us understand the characteristics of OSINT and the challenges like how to improve SNR for poor quality OSINT data.

Anomali ThreatStream is a leading threat intelligence platform which can effectively mitigate such challenges at scale thanks to the largest repository of AI curated global threat intelligence.



The Anomali Threat Research Team

Rishikesh Bhide

Rishikesh Bhide is the Manager, Cyber Intelligence Engineering at Anomali. He has 11+ years of experience in cybersecurity and has worked as research engineer at Symantec, Qualys and now working at Anomali for the past 3 years. Rishikesh and his team responsible for collection, curation and ingestion of Anomali Premium & Anomali Curated OSINT into ThreatStream as well as developing and managing Anomali Targeted Threat Monitoring service and Anomali FS-ISAO trusted circle. Rishikesh also drives the data science strategy for Macula.

Kyle Campbell

Kyle Campbell is an Intelligence Engineer at Anomali, where he has been employed for the past year. Kyle is responsible for feed creation and ingestion of OSINT and premium data, ensuring quality across the entire intelligence lifecycle in addition to utilizing analytics to understand and improve upon trends and gaps in intelligence coverage. Kyle holds a bachelor's degree in Digital Security and Forensics and is Mitre Att&ck Defender (MAD) certified.

Jason Zhang

Jason Zhang is the Director of Cyber Intelligence at Anomali. As a highly motivated cyber threat researcher and a proven product and technology pioneer, Jason has a wealth of experience in technology and product R&D. Prior to joining Anomali, Jason worked at VMware, Lastline, Sophos, Symantec and MessageLabs, specialising in cutting-edge research and automation in threat detection and intelligence analysis. Jason is a regular speaker at leading technical conferences including Black Hat, Virus Bulletin and InfoSec. Jason earned his Ph.D. in signal processing from King's College London & Cardiff University in the UK.

ANOMALI

Website: www.anomali.com   Contact Us: **+1 844-4-THREATS** (847328)

+44 8000 148096 (International Toll-Free)

Anomali is the leader in global intelligence-driven cybersecurity. Our customers rely on us to see and detect threats, stop breaches, and improve the productivity of security operations. Our solutions serve customers around the world in every major industry vertical, including many of the Global 1000. We are a SaaS company that offers native cloud, multi-cloud, on-premises, and hybrid technologies. As an early threat intelligence innovator, Anomali was founded in 2013 and is backed by leading venture firms including Google Ventures, IVP, General Catalyst, and several others. Learn more at www.anomali.com.

808 Winslow Street, Redwood City, CA 94063