White Paper

Managed Intelligence™

Transitioning Cyber Threat Information to Actionable Threat Intelligence Provides Critical Context

Major organizations with significant intellectual property and brand name reputation face a constant onslaught of targeted cyber attacks and information operations campaigns, but often lack the capability to attain context-based attribution - the ability to define the how and the why behind an attack. Such organizations face scenarios ranging from opportunistic threats to financially motivated hackers, state sponsored actors, and even corporate espionage firms.

It often falls on the shoulders of an organization's security operations center (SOC) to sift through high volumes of information and indicators - noise comprised of both legitimate and potentially malicious traffic and signals.

Upon discovery of a potential threat, the security team will be required to determine if a certain attack rises to the level of sophistication to investigate more thoroughly.

Conducting swift and informed external triage using cyber threat feeds and open-source analysis, SOCs can transition data to actionable threat intelligence that provides context on threat actor goals and degree of sophistication.

Peeling the Onion on Technical Infrastructure and Attacker Behavior

The industry has defined 'attribution' as an exercise to identify the true person or entity responsible for an incident. The majority of victims simply want the actor out so they can continue to focus on normal operations.

More mature security teams, however, have a critical need to understand if the attack was targeted versus opportunistic, to understand motivations, and to capture any indicators of compromise (IOC) found beyond their network edge.

Those needs require specialized knowledge of attackers, their tactics, techniques, and procedures (TTPs), geopolitical context, and access to data sources. Analytical rigor is required to sift through significant noise related to normal and innocuous internet activity to identify relevant actors' actions, attributes and infrastructure.

Often what we look for are lapses in operational security by the threat actors, which include but are not limited to the following:

- An actor registered a domain and failed to enable private registration before correcting their mistake.
- An actor forgot to use their VPN or proxy to connect to their C2 infrastructure and revealed their source IP range.
- An actor reused certificates on different infrastructure or failed to properly encrypt their C2 traffic.

All of these lapses in operational security result in artifacts and those are the threads that can provide IOCs outside of the company network. The bad actor(s) made a mistake that is publicly exposed, such as buying a domain that correlates to an originating IP address, and from there a SOC can investigate that domain to review for related internet infrastructure like other domains and IP addresses.

Recognizing a threat actor group is more than a fancy name and location, we focus on identifying the software, internet infrastructure, traffic profile, administrative actions, people, and motivations. Research into internet infrastructure comprises a deep dive into threat information sources, web reputation data, netflow, domain registration data, dark web forums, and other technical data.

Pivoting to Actionable Threat Intelligence

We have observed distinct teams within threat actor groups supporting various activities that contribute to their overall mission to gain access, maintain that access, and collect and exploit data of significance. We have observed a single team that handles the procurement and operations and maintenance (O&M) of infrastructure and another team that handles the day-to-day operation of that infrastructure.

For example, a financially motivated threat actor developed a unique command and control (C2) tool designed to steal financial data. That actor then had a separate team procure the domains, build the infrastructure, and administer the tool. Another team played a traditional sales and marketing role and brought on third-parties to license use of the C2 tool.

But even the most sophisticated teams make mistakes - domain registration, VPN and firewall issues, repeatable but identifiable processes, and common infrastructure - that help give clues to enable context-based attribution. Going a step further, we pivot from the technical analysis to open source intelligence (OSINT) to add valuable context to the nature of the threat an organization faces.

By exposing network infrastructure and drawing associations using threat information and other technology-enabled OSINT connections, we can determine the motivation and sophistication of the threat. We assess characteristics such as:

- Content, stylometric attributes, and similarities between criminal persona accounts and true-name accounts.
- Re-use of content in a spearphish that was similar to content existing elsewhere, such as blog or social media posts.
- Re-use of usernames or email addresses to register a malicious domain or subscribe to a third-party file server or virtual private server.
- Photographs that provide traceable location details such as landmarks or geographical attributes.
- Screenshots, files, or photos used by the actor that leave vital forensic clues revealing real identity or location.
- Details ascertained through direct engagement with the threat actor.

For example, given a physical location, we can often identify internet gateways and leverage various datasets to analyze the location against technical indicators such as device identifiers. This can lead to the identification and sometimes motivations of individuals. From investigations into those individuals we can derive their associations to include circles of trust and employers. Internet gateway information is particularly useful when combined with our ability to query netflow data for the gateway's IP address and analyze the contextual traffic data for additional leads.

Using technical investigations to provide important context and quickly pivot to actionable threat intelligence allows a security team to prioritize steps to improve defensive posture. In addition, context-based investigation allows the security team to derive additional threat intelligence and attack signatures external to their network that will identify coverage gaps and more readily identify future attacks. For sophisticated security teams, the ability to provide this level of detail allows them to educate the broader business about the threats it faces and inform business decisions incorporating a clear and authoritative understanding of risk. This article is the first in a series providing context to threat information that should lead to actionable outcomes in support of the business.

For additional information, visit www.nisos.com or contact info@nisos.com.