Reducing Risk with Intelligence

The Weakness of General Intel

Phishing is the attack vector in nine out of 10 data breaches.[1] Early knowledge about the details of these attacks can dramatically reduce the time to discover a threat in your organization, minimize the threat's effectiveness and diminish the time to respond. Despite this fact, many solutions focus intelligence efforts further down the attack chain attempting to use nonspecific sources of data to combat a very focused threat. Because of this, the global median time from compromise to discovery is still almost 100 days.[2]

Executive Summary

Cybersecurity Solution: Phishing threat intelligence

Challenges: Threat data collected only by machines or systems can be overwhelming, nonspecific and unreliable, making it difficult for incident response teams to quickly and accurately understand risks and address real threats.

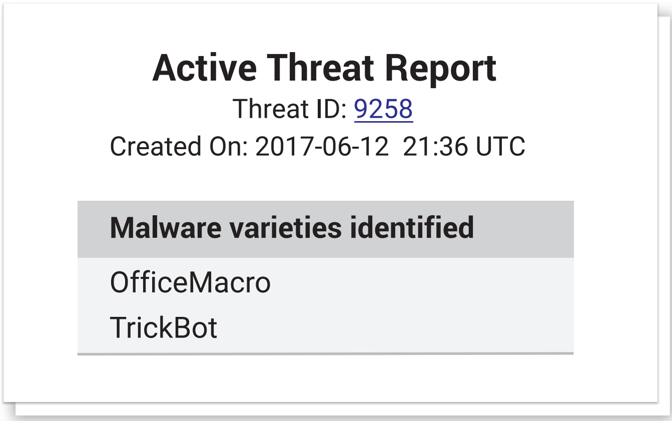
Solutions: Human-vetted, phishing-specific intelligence is the most effective way to yield actionable data to address threats.

Takeaways: Threat intelligence is only actionable if it's timely, relevant, accurate and consumable.

This report explains why threat intelligence must be timely, accurate and consumable to be actionable and that highly relevant intelligence can only be derived from a human-driven process.

Quality Over Quantity

While many organizations recognize phishing as serious, they often struggle to obtain quality information about specific threats. Intelligence feeds built entirely through automation can introduce large amounts of extraneous information and make it difficult to identify real threats within a mass of materials.



Active Threat Report

Threat ID: 9258

Created On: 2017-06-12 21:36 UTC

Malware varieties identified
OfficeMacro
TrickBot

As a result, large amounts of human capital are expended searching through mountains of threat data. Consequently, by the time actionable information is located, the relevant threat information is either stale or the attack has already transpired and data compromise has potentially occurred.

> "Cofense identifies threats before others do. We can see what the malware is and clean it up based on the reports and analysis Cofense sends us."
>
> **— Cyber Intelligence Researcher, Global Retailer**

Making Threat Intelligence Actionable

To get the most use out of threat data collected, it should be:

TIMELY – It's important to find malware as soon as possible, to reduce dwell time. The less time an attacker has inside your infrastructure, the less overall damage he'll be able to inflict.

RELEVANT – Intelligence content needs to provide specific information that's useful to defenders' security stack, so it can be implemented to block or mitigate an ongoing attack. If the data isn't relevant, it simply becomes more noise for the security practitioner to sift through.

ACCURATE – As many new sources of intelligence become available, the ratio of accurate data to information can become compromised. Automated solutions can scrape up data sets that provide incorrect information; and if not vetted properly, the data can introduce false positives. This creates more work for a security analyst—prolonging response times and increasing the damage inflicted by an attacker.

CONSUMABLE – All attack data, such as indicators of compromise (IOCs) and techniques, tactics and procedures (TTPs), will have little actionable value if it cannot be consumed by complementary technologies. These tools include threat intelligence platforms and security information and event management products. To achieve the greatest benefit of defense in depth, layered security should be able to easily consume threat data and implement accurate results immediately.

Only when all of these attributes are accounted for does the intelligence become **ACTIONABLE**.

+
+
+
=
ACTIONABLE

Actionable intelligence is driven by proper context, as not all threats require the same response. Cofense Intelligence provides important context to drive decision-making, allowing responders to select the correct course of action based on attributes of the malware, such as when and where to act first. Response to ransomware should not be the same as a remote access tool; but without the supporting information, responders can find it difficult to assess the threat and know how to begin.

Cofense Intelligence: Human-vetted, Phishing-specific

Cofense Intelligence™ is collected from numerous remote sensors and compiled into vast collections that are then vetted by humans for the greatest accuracy. While there are many different providers of generalized threat intelligence, Cofense Intelligence specifically targets phishing threats to provide the greatest level of relevance and focus on the largest culprit of breaches.

Additionally, Cofense® develops out-of-the-box integrations with partners like SIEM, network and endpoint security, and Threat Intelligence Platform (TIP) vendors. This enables rapid integration without any coding.

> “With the amount of phishing going on currently, especially in retail, we cannot afford to let any of that get through. Cofense Intelligence is absolutely worth it.”
>
> **— Cyber Intelligence Researcher, Global Retailer**

Cofense Intelligence is also provided via a RESTful API to access machine-readable threat intelligence (MRTI) in STIX, JSON and CEF formats for integration with most security applications and other technology platforms. These integrations are seamless and speed return on investment.

Additionally, full reports are available via a web-accessible portal, API, and email delivered in either PDF or HTML. Active Threat Reports contain detailed breakdowns of attacker infrastructure and methodology and put related indicators of compromise in context to help your team understand the attack and respond more effectively. Strategic Analysis Reports provide insight into current phishing trends and tactics by monitoring evolving TTPs.

Conclusion

Modern phishing attacks come from a variety of sources and use sophisticated infrastructure and delivery methods to achieve results. Combatting the attacks requires actionable intelligence – meaning it’s timely, relevant, accurate and consumable. The result is that defenders can spend less time on research and more time focused on mitigation because they can quickly quantify the threat and the risk to the organization.

For more information about this whitepaper or Cofense’s award-winning phishing defense solutions, please email info@Cofense.com. Sign up for Cofense Threat Alerts for updates on the latest malware and ransomware attacks in real-time.

[1] Cofense, “Enterprise Susceptibility and Resiliency Report,” 2016.

[2] Mandiant, “M-Trends 2017: A View From the Front Lines,” 2017.

COFENSE

For more information contact:

W: cofense.com/contact T: 703.652.0717
A: 1602 Village Market Blvd, SE #400 Leesburg, VA 20175