Stamus Networks Launches Free Threat Intelligence Feeds for Newly-Registered Domains

Collection of feeds helps Suricata users identify domains that could be used to host malware and provide infrastructure for various cyber attacks

LUXEMBOURG (Hack.Lu 2023), October 17, 2023 – Stamus Networks, the global leader in Suricata-based network security, today announced the availability of free threat intelligence feeds for newly-registered domains (NRD) that empower Suricata users with increased visibility into potential threats and enhanced data when investigating incidents. Announced at the Hack.Lu conference in Luxembourg – an annual event focused on computer security, cryptography, privacy, and hacking – Suricata users can subscribe to the feeds for free. This is the latest example of Stamus Networks' rich history of developing and supporting open-source technologies including SELKS and the lateral movement ruleset for Suricata.

Every day, hundreds of thousands of new domains are registered. While many support legitimate new websites, brands or products, others are set up by criminals or rogue nation states working to create the infrastructure needed to host malware and command and control access points. Highly targeted organizations, including government institutions, financial services firms, military operations, critical infrastructure operators and more, monitor their network for communications with these newly registered domains as a key part of their cyber defenses.

However, security analysts currently lack an efficient method to collect and analyze this information since it is dispersed across more than 2,400 domain registrars worldwide. Stamus Labs, the company's dedicated threat research team, has created six threat intelligence feeds optimized for Suricata that aggregate and consolidate newly registered domains and are known as the "Open NRD Feeds." Updated daily, this streamlined source of threat intelligence includes several lists:

- **All newly registered domains:** a complete list of all domains that have been registered during the previous 14 or 30 days along with the custom Suricata rule used to enable the list.
- **Newly registered high-entropy domains:** a list of domains that have been registered during the previous 14 or 30 days which exhibit high entropy or randomness along with the custom Suricata rule used to enable the list.
- **Newly registered phishing domains:** a list of domains that have been registered during the previous 14 or 30 days which are designed to mimic the most popular domains. This feed also includes the custom Suricata rule used to enable the list.

"Newly registered domains are a key launching point for malware and other cyber-attacks, but the sheer volume of new domains created each day, spread across thousands of domain registrars, make it overwhelming for security teams to properly track and analyze," said Peter

Manev, chief strategy officer of Stamus Networks. “Supporting defenders is one of our core principles, and by contributing to the open-source community through these free tools, we believe we can help more defenders stop attacks in their tracks.”

To learn more about the Open NRD feeds and to sign up for free, please visit https://www.stamus-networks.com/stamus-labs/subscribe-to-threat-intel-feed. Explore additional open-source contributions and free tools from Stamus Networks here.

About Stamus Networks

Stamus Networks believes in a world where defenders are heroes, and a future where those they protect remain safe. As organizations face threats from well-funded adversaries, we relentlessly pursue solutions that make the defender's job easier and more impactful. The global leader in Suricata-based network security solutions, Stamus Networks helps enterprise security teams know more, respond sooner, and mitigate their risk with insights gathered from cloud and on-premise network activity. Our Stamus Security Platform combines the best of intrusion detection (IDS), network security monitoring (NSM), and network detection and response (NDR) systems into a single solution that exposes serious and imminent threats to critical assets and empowers rapid response. For more information visit: stamus-networks.com.

###

Media Contact:
Chris Ferreira
Three Rings Inc.
860-604-0298
Cferreira@threeringsinc.com