Nominum
Shaping the New Internet

DATASHEET

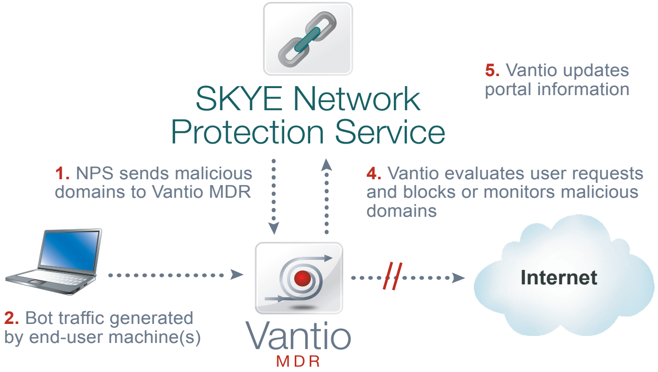
SKYE℠ Network Protection Service (NPS)

PROTECTION FROM BOT-RELATED MALICIOUS ACTIVITY

SKYE™
by Nominum

A key challenge for network owners is minimizing the impact of infected devices on their networks. Bots infest end user machines and send spam or launch DDoS attacks. This unwanted traffic clogs and disrupts networks where it originates and typically traverses many other networks. When other network owners are impacted by this traffic they take action accordingly – all the way up to blacklisting the source. The result is legitimate traffic is affected and applications become unreliable, causing a poor end user experience. End users may also react to these kinds of problems with support calls because they do not realize that the network (or their machines) is running slowly due to an infection. This increases costs.

Nominum Global Network



1. NPS sends malicious domains to Vantio MDR

2. Bot traffic generated by end-user machine(s)

3. Vantio MDR checks requests against lists and blocks malicious domains

4. Vantio evaluates user requests and blocks or monitors malicious domains

5. Vantio updates portal information

Bad traffic created by bots and other malware is not something network owners should have to just live with. Built on proprietary systems developed at **Nominum**, **SKYE** Network Protection Service (NPS) provides a real-time feed of bot-related malicious domains that allows the botnet threat to be managed (block, monitor, record, report). NPS, together with Nominum Centris™ threat aggregation and provisioning server and the Vantio™ Intelligent DNS System running Malicious Domain Redirection (MDR) policy software module, can limit bot-generated traffic and curtail propagation of botnets and other kinds of malware.

Data contained in NPS is categorized by threat level and instantly and automatically served over secure connections to **Centris** servers, where it is distributed to instances of **Vantio** MDR. Vantio MDR evaluates incoming DNS queries in real time and makes decisions about trustworthiness of requested destinations based on policies established by the network owner. Web sites can also be placed in a special whitelist category that is never blocked. A high degree of automation coupled with aggregation provided by Centris, allows the solution to scale to tens of millions of end users and literally hundreds of millions of domains with no impact to the network or DNS performance.

The need to protect the network can not intrude on the Internet experience. It cannot introduce additional delay or reduce network reliability. It also can not violate user privacy. Nominum's solution for protecting networks does not introduce any new equipment into the network or change the underlying architecture. There is no change in network performance or latency and no change in DNS performance or reliability. Because there is no need to examine end user interactions over the Web (packet inspection of transactions between client software and Web destinations) there is no invasion of end user privacy.

KEY FEATURES

- Real-time, proprietary DNS data repository for bots and bot-related activity
- Worldwide network of installed DNS for botnet discovery
- Dynamic identification and classification of network level threats
- Secure provisioning and propagation from NPS to Nominum Centris and Vantio MDR
- Advanced validation algorithms to minimize risk of false-positives
- Automated up-to-the-minute updates to protect against fast-changing attacks
- Integration with Vantio MDR provides "turn-key" network protection
- Integration with Vantio UAR for device quarantine and remediation
- Multiple modes of enforcement-discover, monitor, block
- Secure and open APIs for secondary data sources

Comprehensive Threat Coverage

The algorithms used in NPS were developed by researchers at Nominum using data covering tens of millions of threats gathered over Nominum's global network from across the Internet. All threat information is completely validated to ensure the service is highly effective without introducing false positives that will degrade the user experience.

NPS Data Categorization Enables Different Service Modes

Nominum algorithms separate NPS threat data into categories. Categorizing threat data enables different service modes. For example,with separate data categories network owners can treat requests for domains in a Block category that are confirmed bad, differently from requests for Web destinations in the suspected bad Monitor category. It also allows the behavior of threat domains to be studied over time to develop a deeper undestandintg of how threats propagate and evolve. In the future categories will be extended so additional service modes can be implemented.

Vantio MDR Leverages Data Categorization

MDR can enforce different policies when DNS queries match different SKYE Network Protection Service categories. Categorized data from NPS is automatically served over secure connections across the Internet to network owners. In-network MDR policy software is configured with service modes to reflect the different NPS categories. For instance, attempts to reach Web resources in the Block category can be blocked or redirected by MDR.

Alternatively network owners can choose to simply log attempts to reach destinations in the Monitor category as part of a network evaluation to gain a better understanding of the types and quantities of infections on their network.

NPS will also track and log requests for domains in a Monitor category. The data gathered is useful for assessing suspected threats by observing activity in a live network setting over time. This additional data gathering capability forms the basis of Adaptive Learning and leads to continuous improvement in threat protection.

Advanced Algorithms Maximize Data Accuracy

The need to protect the network can not intrude on the end user Internet experience. Nominum has invested heavily in engineering resources and infrastructure to build a highly reliable and effective network protection service. Researchers at Nominum take advantage of a global network of threat data sources and use advanced algorithms to validate threat data.

World Class Network

SKYE NPS is provisioned on Nominum's network which is based on a highly redundant meshed design that employs high bandwidth circuits from multiple Tier-1 ISPs. Services are situated in carrier grade data centers with fully-redundant, industry-best networking elements. At each site NPS is hosted on multiple servers behind the latest generation load balancers. Three layers of protection against DDoS are built into the network itself.

NETWORK OWNER BENEFITS

- Protection without the risks of intruding on privacy
- Completely automated network threat protection
- One-stop source for accurate up-to-the-minute threat data
- Off-network analysis and objective threat determination
- Reduces network and carrying cost associated with malicious traffic
- Reduction of outbound spam and other abusive activity
- Improved network reputation
- Neutral appeals process for claimed false positives
- Event tracking and reporting allows easy communication with external parties
- Brand differentiation and corporate responsibility

END USER BENEFITS

- Protection against bot-related threats (e.g. identity theft, spying, etc.)
- Ensures devices and applications are not being leveraged as part of a bot network
- Ensure bot-related activity does not interfere with user activity
- Faster Internet—reduces impact of bot-related activity on all users
- More value from their Internet service
- Universal protection across every device in the home
- Zero downloads—network-based actions eliminate user burden
- Zero configuration—eliminates user error