TECH TALKS: SUPPORTING THE REMOTE WORKFORCE

Threat Hunting Techniques For Today’s Biggest Threats
PANELISTS TODAY

Host: Brad Six
Technical Product Evangelist

Guest Speaker: Mark Brooks
VP Customer Solutions

- Enter comments anytime via Q&A Window at the bottom
- All Tech Talk recordings are here - https://www.graylog.org/tech-talks/s1
As Remote Work Becomes the Norm, Security Fight Moves to Cloud, Endpoints

A majority of firms expect to keep more employees working remotely post-pandemic, forcing businesses to undertake more comprehensive digital and cloud transformations.

Summary of Attacks

APT groups are using the COVID-19 pandemic as part of their cyber operations. These cyber threat actors will often masquerade as trusted entities. Their activity includes using coronavirus-themed phishing messages or malicious applications, often masquerading as trusted entities that may have been previously compromised. Their goals and targets are consistent with long-standing priorities such as espionage and "hack-and-leak" operations.

Cybercriminals are using the pandemic for commercial gain, deploying a variety of ransomware and other malware.

Both APT groups and cybercriminals are likely to continue to exploit the COVID-19 pandemic over the coming weeks and months. Threats observed include:

- Phishing, using the subject of coronavirus or COVID-19 as a lure,
- Malware distribution, using coronavirus- or COVID-19-themed lures,
- Registration of new domain names containing wording related to coronavirus or COVID-19, and
- Attacks against newly—and often rapidly—deployed remote access and teleworking infrastructure.
NOW ONSTAGE: Threat Intelligence

Couple of Options
- Graylog Threat Intelligence Plugin
- 3rd Party Threat Intelligence Feed

Preparing Log Data
- Choose which log event sources you want to compare against
- Identify the fields to use for comparison
- Normalize field names
- Select streams to be included in lookup processing
Graylog Threat Intelligence Plugin

- IOC Lookups
  - Tor exit nodes
  - Spamhaus
- Enable in System/Configurations -> Plugins
- Simple integration with Pipeline Rules

https://www.graylog.org/post/integrating-threat-intelligence-into-graylog-3
Graylog Threat Intelligence Plugin

Graylog Threat Intelligence Plugin

- IOC Lookups
  - Tor exit nodes
  - Spamhaus
- Enable in System/Configurations -> Plugins
- Simple integration with Pipeline Rules

https://www.graylog.org/post/integrating-threat-intelligence-into-graylog-3
Graylog Threat Intelligence Plugin

- IOC Lookups
  - Tor exit nodes
  - Spamhaus
- Enable in System/Configurations -> Plugins
- Simple integration with Pipeline Rules

https://www.graylog.org/post/integrating-threat-intelligence-into-graylog-3
Graylog Threat Intelligence Plugin

- IOC Lookups
  - Tor exit nodes
  - Spamhaus
- Enable in System/Configurations -> Plugins
- Simple integration with Pipeline Rules

https://www.graylog.org/post/integrating-threat-intelligence-into-graylog-3
Threat Intelligence Subscriptions

Variety of options for log enrichment

- IP Address/Domain Name Reputation
- Hash Values - Malware
- WHOIS Data
- GeoIP

Leveraged in the Processing Pipelines (lookup tables)

Supported Formats – CSV, DSV, OTX API, HTTP JSON path, DNS Lookup

Leveraging 3rd Party Feeds

Lookup Tables Are amazingly powerful

Create a Data Adapter

System/Configuration → Lookup Tables → Data Adapters

Sets the type, path, update interval, delimiter, key and value
Leveraging 3rd Party Feeds

Lookup Tables Are amazingly powerful

Create a Cache

System/Configuration → Lookup Tables → Caches

Sets the type, maximum entries and expiration
Leveraging 3rd Party Feeds

Lookup Tables Are amazingly powerful

Create the Lookup Table
System/Configuration → Lookup Tables

Links the Data adapter with the Cache
Defines “unknown” Lookups
Leveraging 3rd Party Feeds

Lookup Tables Are amazingly powerful

Create Pipeline Rules
System/Configuration → Pipelines

Creates the lookup step as part of log processing
Creating a Notification

Create an Alert

Alerts → Alerts & Events

Sets the filter criteria based on a successful lookup value
QUESTIONS?

- TechTalks@graylog.com

FOLLOW US

- Twitter: @graylog2
- Linkedin: Graylog
- Reddit: /r/graylog/
BUT WAIT, THERE’S MORE!

More Tech Talks to Come in the Near Future

SPECIAL PRICING ON 10GB & 20GB PACKAGES WITH JUMP START SERVICES