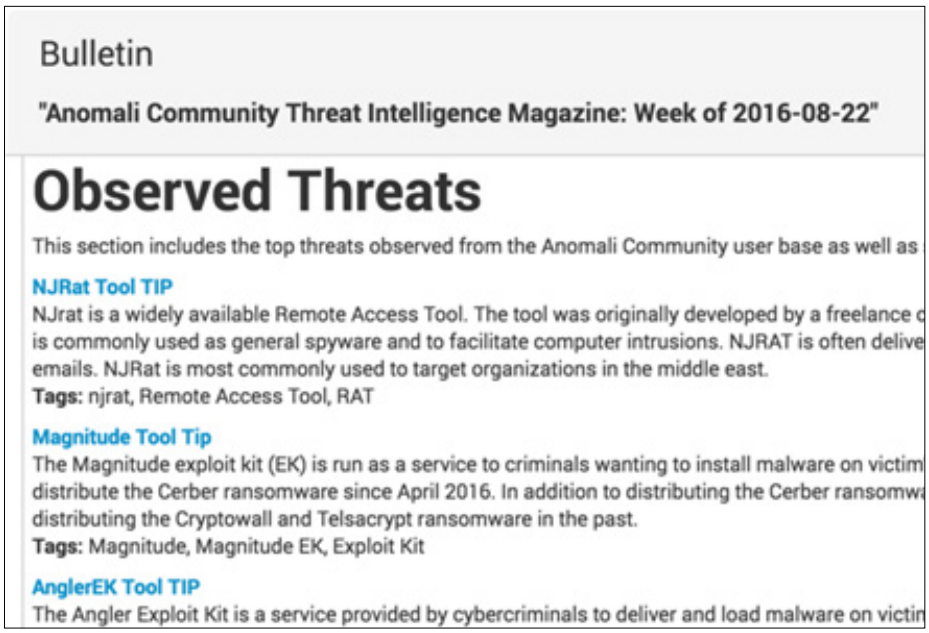
Anomali ThreatStream Community App for Splunk

The Anomali ThreatStream Community App for Splunk brings together Anomali's rich threat intelligence with Splunk's deep analytics to help organizations identify and response to external security threats.

The Anomali Weekly Threat Briefing

Every week the award winning Anomali Labs team publishes a threat briefing, delivering topical cyber events and intelligence to subscribers. The briefing includes trending threat information and new threat intelligence. Anomali also provides details on observed threats across the global Anomali ThreatStream community. All the research is vetted and curated by the Anomali Labs team and includes actionable IOCs and detailed threat bulletins.



Bulletin

"Anomali Community Threat Intelligence Magazine: Week of 2016-08-22"

Observed Threats

This section includes the top threats observed from the Anomali Community user base as well as

NJRat Tool TIP

NJrat is a widely available Remote Access Tool. The tool was originally developed by a freelance c
is commonly used as general spyware and to facilitate computer intrusions. NJRAT is often delive
emails. NJRat is most commonly used to target organizations in the middle east.

Tags: njrat, Remote Access Tool, RAT

Magnitude Tool Tip

The Magnitude exploit kit (EK) is run as a service to criminals wanting to install malware on victim
distribute the Cerber ransomware since April 2016. In addition to distributing the Cerber ransomw
distributing the Cryptowall and Telsacrypt ransomware in the past.

Tags: Magnitude, Magnitude EK, Exploit Kit

AnglerEK Tool TIP

The Angler Exploit Kit is a service provided by cybercriminals to deliver and load malware on victi

In addition to the weekly briefing, Anomali also provides Breaking News alerts delivering critical updates in real time as new cyber threats become known. This information is delivered proactively to Splunk app users with all available details to evaluate if customers have been breached.

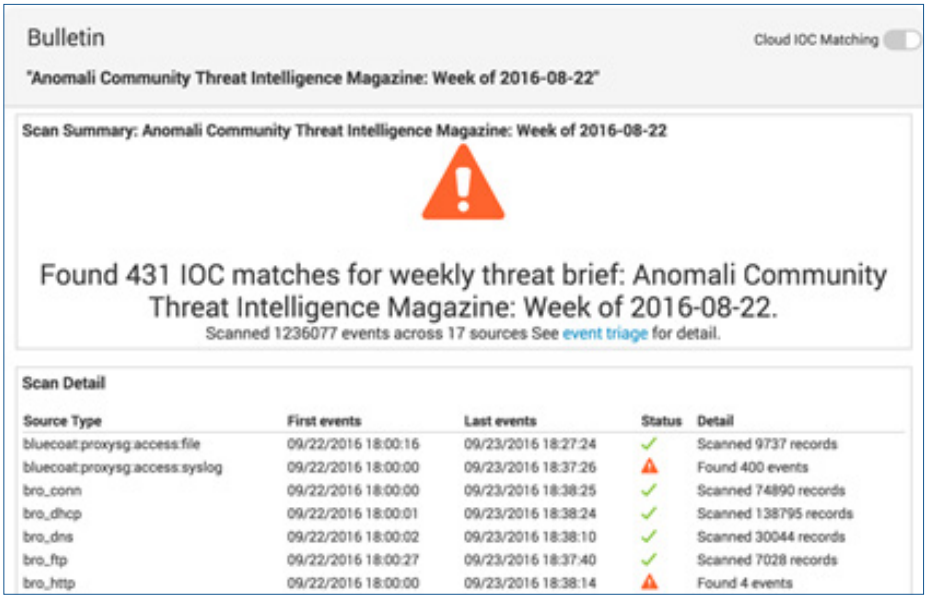
This service allows independent threat researchers to publish and share intelligence research with the Anomali ThreatStream community. Anomali makes intelligence sharing efficient and seamless, allowing the entire community to benefit from threat analysis from any member

2317 Broadway, 3rd Floor, Redwood City, CA 94063 USA
1-408-800-4050 | info@anomali.com | www.anomali.com

ANOMALI™

Automated Health-Check

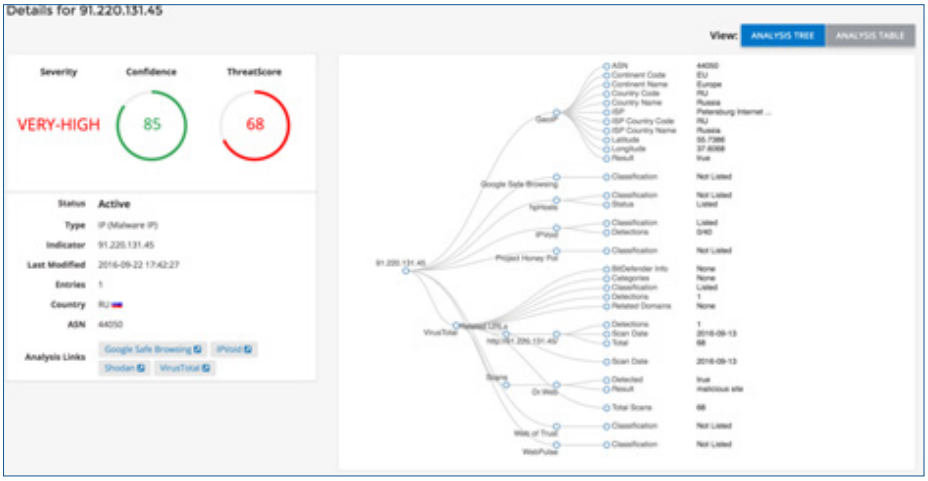
Anomali takes the intelligence sharing further by allowing subscribers to instantly check their exposure against published threats. Anomali briefings include specific, actionable IOCs and automate a health check against subscribers' own live Splunk event data.



The health-check allows users to evaluate their security posture against the Anomali Weekly Briefing, any Breaking News updates, and any shared intelligence from the Anomali ThreatStream community.

Investigate and Respond

Once threat matches are identified Anomali provides security teams the tools to research and investigate IOCs further. Here Anomali delivers critical insight into IOC threats, including actors, techniques, associated IOCs and other threat details. From within the Splunk interface users can access this information, or pivot to the Anomali portal for additional investigation capabilities.



For Splunk ES customers Anomali pushes IOC notable events directly into the ES interface. From here users can expand entries in the Splunk interface, revealing in-depth details about the event.

ANOMALI™

2317 Broadway, 3rd Floor, Redwood City, CA 94063 USA
1-408-800-4050 | info@anomali.com | www.anomali.com