Retina IoT (RIoT) Scanner

Keep Your IoT Devices From Getting Out of Control

BeyondTrust
VISIBILITY. KNOWLEDGE. ACTION.

In the simplest terms, the Internet of Things (IoT) is an increasingly massive ecosystem of connected devices. Intel and others estimate that, by 2020, 200 billion connected devices will comprise the Internet of Things. That's a whole lot of things!

Because IoT devices are connected to the wild, and to each other, not only are they vulnerable to attack, but the data that they produce and the applications that support them are also potential attack vectors.

IoT Threats Are Evolving

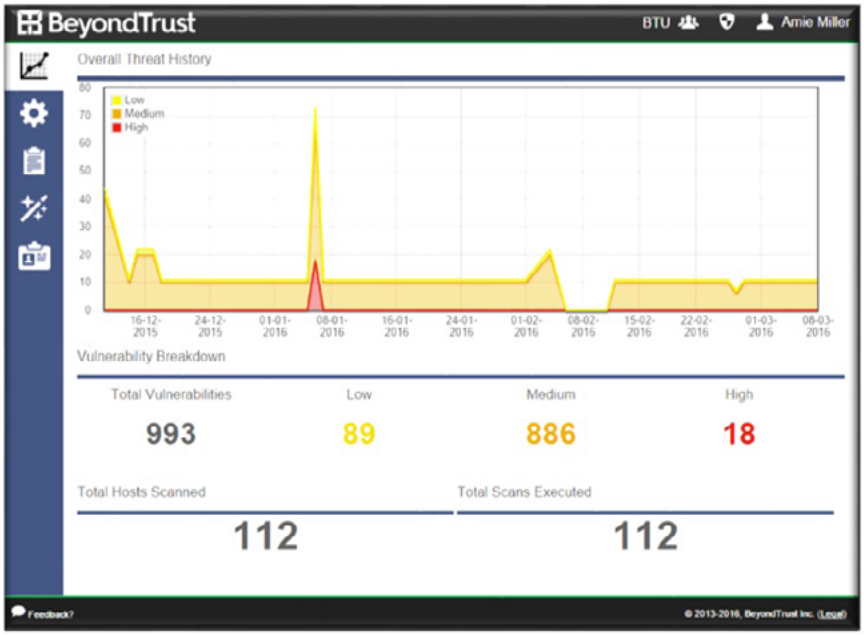
A new generation of distributed denial of service (DDoS) attacks has emerged, representing a significant threat to organizations and governments alike. The most notorious of these being the recent wide-scale DDoS attacks perpetrated by the Mirai Botnet.

Mirai malware continuously scans the internet for vulnerable IoT devices, uses a short dictionary to crack their default passwords, and then enslaves them as part of an IoT botnet attack. To date, Mirai has infected hundreds of thousands of IoT devices, and counting – with the vast majority unbeknownst to their owners.

How can you protect yourself and others from becoming victims of these weaponized "things"?

Manage the Vulnerability of Things

With the Retina IoT (RIoT) Scanner, organizations now have the ability to reliably identify at-risk IoT devices, such as IP cameras, DVRs, printers, routers, and more. Powered by Retina, an award-winning vulnerability scanner trusted by thousands of organizations, and delivered via the simplicity of BeyondSaaS' cloud-based interface, RIoT gives you an attacker's view of your IoT devices and their associated vulnerabilities.



RIoT Dashboard: Historical view of IoT related vulnerabilities over time.

Key Capabilities

With nothing to install, RIoT enables you to quickly identify high-risk IoT devices connected to the wild. Once found, RIoT performs vulnerability assessments, including safely checking for the use of default passwords. Everything you need is pre-configured and delivered through an HTML 5 interface that lets you manage and communicate IoT risk from virtually anywhere. Just point and click and let RIoT do the rest.

Why RIoT?

- Identify high-risk IoT devices
- Safely check for default or hard-coded passwords
- Generate clear IoT vulnerability reports and remediation guidance
- Perform external scans of up to 256 IPs
- Authenticate via Microsoft Live
- Communicate IoT threat history trends
- Unlimited user accounts
- Scheduled or ad-hoc testing
- Encrypted data transmission
- No software or hardware install

BeyondInsight Threat and Vulnerability Intelligence

The Retina IoT Scanner is part of BeyondInsight Threat and Vulnerability Intelligence, which provides centralized management, policy, reporting, and analytics for BeyondTrust PowerBroker privileged access management and Retina vulnerability management solutions. Capabilities include:

- Centralized solution management and control via common dashboards
- Asset discovery, profiling and grouping
- Reporting and analytics
- Workflow and ticketing
- Data sharing between Retina and PowerBroker solutions
- Importing of third-party vulnerability feeds to support multi-scanner and migration scenarios.

With BeyondInsight, IT and Security teams have a single console through which to view user and asset risk.

CONTACT

North America
info@beyondtrust.com

EMEA
emeainfo@beyondtrust.com

APAC
apacinfo@beyondtrust.com

LATAM
latam@beyondtrust.com

CONNECT

Twitter: @beyondtrust
Linkedin.com/company/beyondtrust
Facebook.com/beyondtrust
www.beyondtrust.com

The Insecurity of Things

By design, most IoT devices are "set it and forget it" appliance types that are intended to run mostly unchanged and unmanaged for the entirety of their useful lives. And, as such, they typically lack any built-in security or mechanisms for programmatically making device-level changes.

Some common IoT insecurities include:

- Lack of visibility into sanctioned and shadow IoT devices
- Weak configurations, such as default or common passwords, and unencrypted traffic
- Limited ability for users to update IoT device software, passwords, or settings

Any of these scenarios can spell big trouble for your organization

Stop Your IoT Devices from Going Rogue

Utilizing precise information, such as server banner and header data, RIoT is able to pinpoint the make and model of a particular IoT device. From there, RIoT safely tests whether or not that device is using default or hard-coded credentials for Telnet, SSH, or Basic HTTP Authentication, which are the preferred attack vectors that botnets (most notably, Mirai) initially use to breach a system.

It's worth reiterating that RIoT does not endanger your devices or network by subjecting them to dictionary-style probes, instead RIoT checks a specific set of credentials known to be used by a specific IoT device.

From the cloud, RIoT conducts fast, highly accurate security assessments of your IoT devices, while delivering straightforward and actionable reports. As a result, you're able to quickly identify IoT-related vulnerabilities, clearly understand their potential impact, and decisively act to mitigate threats. Simply specify a target IP or IP range, and RIoT handles the rest.

- Get fast, comprehensive, and accurate scanning, backed by over 15 years of expertise
- Conduct multiple vulnerability assessments after a simple registration process
- Access your account using Microsoft Live two-factor authentication
- Leverage single sign-on via Active Directory and other identity providers
- Eliminate software and hardware deployment and configuration
- Manage job scheduling, results, and reports through a highly secure, encrypted HTML 5 web interface
- Rely on Microsoft Azure's highly secure multi-tenant architecture

In the next few years, the IoT ecosystem will swell to an estimated 200 billion things, add an additional 1 billion users, and increase its data production by a factor of 5. With a labor shortage of cybersecurity pros that's seven figures and counting, more devices, more people, and more data equals more ways in for adversaries.

It's a jungle out there, make sure you get your RIoT gear! www.BeyondTrust.com/RIoT