RISKIQ®

Rackspace Accelerates External Digital Threat Investigation with RiskIQ PassiveTotal®

rackspace®

About Rackspace

Rackspace, the #1 managed cloud company, helps businesses in 150 countries tap the power of cloud computing without the complexity and cost of managing it all on their own. Rackspace engineers deliver specialized expertise, easy-to-use tools, and fanatical support for leading technologies, including AWS, Google, Microsoft, OpenStack, and VMWare.

Challenges

Rackspace's security organization sought a more efficient way to obtain and analyze diverse internet data sets, such as WHOIS information or SSL certificates or domains, while investigating and responding to incidents. With broader and more relevant internet data, they could paint a better picture to leadership to describe how adversaries might invade and use their infrastructure to conduct targeted or broad attacks, and how these and other threats were being mitigated.

Rackspace also looked to automate and speed-up the time-consuming process of identifying, triaging, and responding to external threats with a more robust and unified set of tools for their security team. As such, Rackspace sought a threat intelligence tool that would improve their mean time to detect and respond to (MTTD/MTTR) external threats.

60%	25%	10%
of analysts' time	of senior management's time	of a senior manager for cyber security's time

For many organizations, researching threats can take days and weeks. In some cases, Rackspace could spend upwards of 60% of analysts' time, 25% of senior management's time and 10% of a senior manager's time to respond to a security issue. For example, a phishing attack could take up to an hour to triage and respond, which may involve identifying hosts and employees attacked, removing the phishing email, putting up blocks, and more—often done manually with multiple tools and data sources.

Challenges

The challenges faced by Rackspace in guarding against external threats included:

- Improving processes to find, verify, and respond to external threats to improve staff use and speed response time
- Enhancing defenses against external threats to reduce reputational risks due to cyberattacks, specifically from unknown external threats
- Identifying online brand abuse and domain infringement by competing service providers

Solution Benefits

RiskIQ PassiveTotal has delivered these benefits:

- Automated identification, verification, and response to external threats, lessening staff use and speeding response time
- Assures brand protection through proactive monitoring of domain and brand infringement
- Quickly uncovers attackers' infrastructure, thus allowing a more thorough understanding of the adversary
- Fortifies Rackspace's internal security systems and integrates with other security tools to automate and consolidate once manual actions across multiple systems
- Allows powerful means to communicate results to management

Common with other popular companies, Rackspace's brand was a potential target for typosquatting—variants of its web domain used to redirect visitors who made a typo to a malicious website. During a phishing attack, attackers can create numerous domains with popular brand's name. Rackspace wanted to more efficiently identify newly created Rackspace domain variants and enact preventative measures. By doing so, they would extend means to prevent data theft for its employees and customers, as well as protect their reputation.

As they went out to find a solution, additional key considerations included:

- Ease of deployment and use
- Ability to automate multiple functions through integrations and API
- Consolidated data and alerts, so users didn't have to use multiple systems to study the attack
- Efficient research and threat response collaboration
- Ability to efficiently demonstrate results to company leadership

Solution

Rackspace turned to RiskIQ PassiveTotal®, which expedites external threat investigation attacks and automates threat research collaboration and artifact monitoring, to address its need to quickly identify and respond to external threats.

"PassiveTotal has been extremely helpful for our operations in responding to and preventing attacks," said Gary Ruiz, Rackspace Senior Manager for Cybersecurity. "It is definitely a must-have tool for us from this point forward."

Rackspace found PassiveTotal extremely easy to deploy, implement, and use, and it quickly became apparent that its internet data sets are extensive. Additionally, it meets all of Rackspace's needs for collaboration and alerting security staff on external threat activity of interest. PassiveTotal quickly and automatically pinpoints attackers and their infrastructure to allow Rackspace to learn more about an attacker and quickly deploy preventative measures. Information gathered through PassiveTotal allows Rackspace to learn more about an adversary's infrastructure and identify additional environments being actively attacked. This lets Rackspace prevent future attacks based on observed IOCs regarding new domains or IPs.

Plus, PassiveTotal enabled Rackspace's security team to show leadership what other companies were attacked, so that Rackspace could reach out to these firms to see if they would like to work together toward preventing future attacks.

"The information we could gather with PassiveTotal allowed us to learn more about the adversary's infrastructure, identify additional environments under attack and prevent future attacks based off information regarding new domains or IPs being used," Ruiz said.

"The information we could gather with PassiveTotal allowed us to learn more about the adversary's infrastructure, identify additional environments under attack and prevent future attacks based off information regarding new domains or IPs being used."

– Gary Ruiz, Senior Manager for Cybersecurity Rackspace

Results/Outcome

Overall, RiskIQ's PassiveTotal provided Rackspace with a comprehensive toolset with broad intelligence that offered capabilities to automatically alert the team to threat indicators they were tracking.

In particular, information gathered by PassiveTotal let Rackspace learn more about their adversary's infrastructure and identify additional environments that may be targeted to prevent future attacks. Furthermore, it allowed the firm to efficiently identify domains and competitors infringing on their brand. In many cases, threat investigation takes only minutes leveraging RiskIQ's API, which automates access into and data extraction from PassiveTotal. This operational efficient improves Rackspace human resource utilization, given the considerable cost to find, onboard and develop cybersecurity analysts.

Also, it took only a few days to train Rackspace's security analysts on using PassiveTotal. At the same time, results and information uncovered by PassiveTotal can be used to educate tier-one and tier-two analysts and leadership on threats and how to address them.

PassiveTotal can also identify new domain variants to prevent future domain infringement and phishing attacks. Its ability to identify new threats significantly reduces Rackspace's MTTD (mean time to detect) and MTTR (mean time to respond), thus minimizing possible damage to Rackspace's and their customers' brand reputations through compromise of sensitive data. Meanwhile, PassiveTotal quickly identifies newly created domain variants in phishing attacks, thus allowing Rackspace to proactively block them and prevent future attacks.

Next Steps

Given the great success that Rackspace has had in using RiskIQ's PassiveTotal to quickly identify and respond to external threats, the company plans to expand its use of RiskIQ products for further protection from beyond the firewall. In addition to using API to automate Splunk, Phantom and other data-analysis software, Rackspace expects to automate its own applications through API.

They will also expand the use of PassiveTotal projects to more efficiently communicate info between Tier 1 and Tier 2 support, and also to demonstrate results to management.

Rackspace is exploring the use of RiskIQ Digital Footprint, which identifies a company's external-facing assets—in essence, its entire digital presence—to be fully aware of vulnerabilities to external threats. The company also wants to look at bringing on RiskIQ External Threats, which covers domains, mobile, social and anti-phishing exposures by crawling the internet through virtual user technology.

"PassiveTotal has been extremely helpful for our operations in responding to and preventing attacks. It is definitely a must-have tool for us from this point forward."

– Gary Ruiz,
Rackspace, Senior Manager for Cybersecurity

Conclusion

RiskIQ PassiveTotal is a very effective solution for Rackspace to quickly identify and respond to external threats. Because of PassiveTotal, Rackspace's time needed to research an external threat has been reduced. Likewise, the RiskIQ API's ability to automatically find and identify threats has reduced Rackspace's time spent on triaging and responding to them. As a result, Rackspace has been able to better prevent damage to its employees' and customers' personal information and brand reputation when attacked by external threats.

To further benefit from RiskIQ's capabilities, Rackspace is currently automating the use of Splunk's log data management, Phantom's security automation, and other digital-analysis software through RiskIQ's API, and Rackspace looking to integrate its own applications into the program as well.

Beyond this, the company is exploring the use of RiskIQ Digital Footprint™ and RiskIQ External Threats to further extend their digital threat management program.

RISKIQ®

RiskIQ, Inc.
22 Battery Street, 10th Floor
San Francisco, CA. 94111

sales@riskiq.net
1 888.415.4447

Learn more at riskiq.com