株式会社ラック 様

導入事例

RISKIQ®

過去のIPアドレス／ドメイン名情報をPassiveTotalで迅速に把握し、サイバー攻撃に対応。攻撃者の先手を打つプロアクティブ防御も実現。サイバー救急センター、セキュリティ研究部門での作業効率も格段に向上。

User Profile

LAC

株式会社ラック
所在地：東京都千代田区平河町2-16-1
導入時期：2016年5月
URL：https://www.lac.co.jp/
事業内容：1986年に創業。1995年より情報セキュリティ事業に取り組み、国内初のセキュリティ診断の提供を開始した。現在では同分野のリーディングカンパニーとして、官公庁・企業・団体等の顧客へ、業界屈指のセキュリティ技術に裏付けられた先端のITトータルソリューションサービスを提供している。

サイバー・グリッド・ジャパン
次世代技術開発センター
センター長
小笠原 恒雄 氏

ITプロフェッショナル統括本部
サイバーセキュリティ事業部
サイバー救急センター
石川 芳浩 氏

導入のPOINT

1. サイバー攻撃を調査・解析する上でインテリジェンスツールは必須
2. 情報量が豊富で、操作性に優れたユーザインターフェース
3. 充実したAPIの提供

サイバー攻撃の効率的な調査・解析にはインテリジェンスツールの活用が不可欠

サイバーセキュリティ分野のリーディングカンパニーとして知られるラック。同社は創業以来展開してきたSI事業と、インターネットの利活用の進展に伴い立ち上げたセキュリティ事業をビジネスの柱としており、さまざまな顧客に向けて業界屈指のセキュリティ技術を駆使した先端のITトータルソリューションサービスを提供している。

また同社は、サイバー被害を受けた企業・団体への支援を行う専門組織「サイバー救急センター」と国内最大級のセキュリティ監視・運用センター「JSOC」を運営している。さらに、サイバー攻撃による被害発生を防ぐため、セキュリティ専門家を参集した研究部門「サイバー・グリッド・ジャパン」を2014年に設立。関連技術の研究や人材育成などに取り組んでいる。サイバー・グリッド・ジャパン 次世代技術開発センターセンター長の小笠原恒雄氏は、「このように当社はさまざまな活動を行っていますが、その際、不正サイトなどの脅威を調査・解析する上で、重要な役割を担うのがインテリジェンスツールです」と語る。

インテリジェンスツールは、マルウェア解析やインシデント対応の際に把握した不正通信先のIPアドレス／ドメイン名情報やWHOIS情報を確認し、調査・解析作業を効率的に行うためには不可欠の存在だ。ITプロフェッショナル統括本部 サイバーセキュリティ事業部　サイバー救急センターの石川芳浩氏は「サイバー攻撃を調査・解析する際は、マルウェアが外部通信した相手を調べる必要がありますが、不正サイトの多くはIPアドレスやドメイン名が頻繁に変更されるため、いつ悪用が始まったのか、いつ復活したのかなど過去のIPアドレス／ドメイン名情報をある程度は把握しなければなりません。特に近年は脅威が変化するスピードも速まっており、インテリジェンスツールの必要性が高まっていました」と説明する。

こうした中、「Passive DNS」と呼ばれる手法の有効性が次第にアナリストの間で注目され始めた。Passive DNSにより、DNSサーバー間の通信を受動的に記録しモニタリング・調査することで、IPアドレスとドメイン名の関係について変化を確認することが可能だ。具体的には、Passive DNSを利用することで、把握するIPアドレスやドメイン名情報をもとに、攻撃者が関与する他の不正サイトをあぶり出すことができる。「当社では2013年ごろから本格的に解析作業での活用を行うようになりました。優れたツールを探している中で知ったのが、米国RiskIQ社が提供する脅威分析ツール『PassiveTotal』だったのです」（小笠原氏）

無償版の利用でその効果を実感 豊富な情報量と優れた操作性、充実のAPIを評価

PassiveTotalは、独自に収集したDNS情報やWHOIS情報等のデータを蓄積し、多角的な脅威分析を可能にするSaaS型ソリューションである。ラックでは当初、日本でPassiveTotalが取り扱われていなかったこともあり、無償版を利用していた。無償版は有償版と比べて一部の

macnica networks

株式会社ラック 様

導入事例

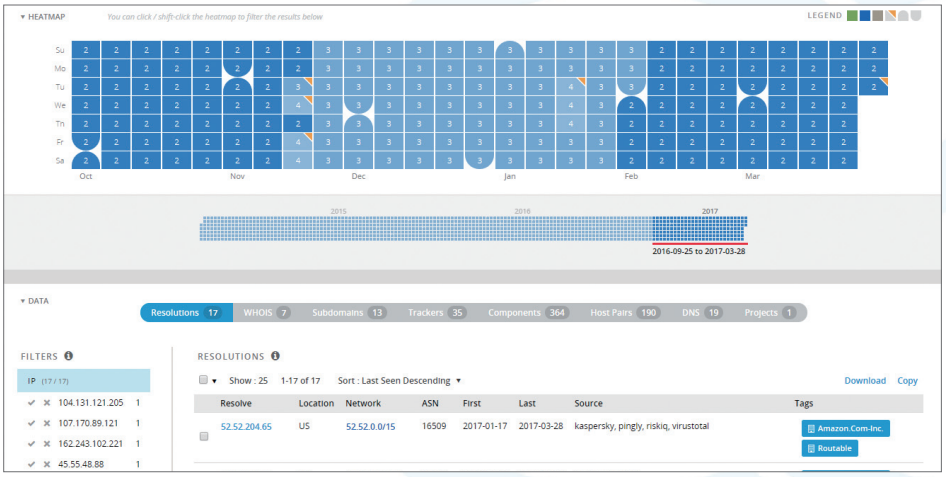
RISKIQ®

機能に制限があるが、それでも脅威の把握や攻撃者を追跡する上で非常に効果的であることを実感したという。

その後、2016年5月にマクニカネットワークスがRiskIQ社と販売代理店契約を締結。日本での取り扱いを開始したことから、ラックは利用に制限のない有償版の導入を決定した。「導入に際しては、他の3～4社のサービスと比較・検討しましたが、PassiveTotalは豊富な情報量と収集対象の幅の広さに加え、ユーザインターフェースが優れていました」（石川氏）

これに加え、単に通信内容が検索できるだけでなく、タグ情報やハッシュ情報、インターネット上にある関連するレポートなども付加してくれる点、APIが充実している点などを評価し、同社はPassiveTotalの導入に踏み切った。「研究者としては調査に際していろいろと試してみたくなるものなのですが、その思いに最も応えてくれそうなのがPassiveTotalだったのです」（小笠原氏）

PassiveTotalの画面



作業効率が格段に向上、大幅な省力化を実現 攻撃者の先手を打つプロアクティブ防御も可能に

現在ラックでは、マルウェア解析者、スレットインテリジェンスアナリスト、スレットインテリジェンスプラットフォーム開発エンジニアの3名が、所属するグループでPassiveTotalを利用している。

このうちマルウェア解析者は、不正なドメイン名やIPアドレスの調査にPassiveTotalを使っている。この解析を通じて作成された脅威の情報は、ラックが提供する各サービスにおいて活用されているという。

一方、スレットインテリジェンスアナリストは、主にアトリビューション活動（攻撃者の特定）で活用しており、具体的には攻撃者の手法を解析したり、特定の脅威やマルウェアをテーマにした調査解析などに使ったりしているとのことだ。

そしてスレットインテリジェンスプラットフォーム開発エンジニアは、主に「サイバー・グリッド・ジャパン」での研究に活用しており、同社が蓄積している脅威情報の充実などに役立てている。さらに、研究所におけるアナリストの活動を支援するための環境整備、つまり解析を迅速かつ容易にするインテリジェンスプラットフォームの構築にも取り組んでいるという。

「PassiveTotalの導入により、作業効率が格段に向上し、大幅な省力化を実現しました。加えて、Passive DNSだけでなく、WHOIS情報の蓄積にも対応するなど機能も充実してきており、より活用の幅が広がっています」（石川氏）

もう一つの大きな効果は、攻撃者の先手を打つ方法を、対策側が持つことができた点だという。

「PassiveTotalはプロアクティブ防御の実現にも大きく貢献しています。PassiveTotalの活用により、今後悪用される疑いがあるIPアドレスやドメイン名にも注目できるようになりました」（小笠原氏）

他のツールとも連携させ 新たなソリューションの提供に活用

今後、ラックではPassiveTotalを活用した新たなソリューションの提供を目指すとのことだ。小笠原氏は「他のソリューションと連携させることで、自動的にプロアクティブ防御を行えるサービスを実現したいと考えています」と抱負を語る。

独自で開発しているアナリスト支援システムにPassiveTotalを組み合わせれば、さまざまな収集データをもとに、自動的に脅威を検知・調査・解析を実現することができる。これで適切な対応が可能になり、情報システムの保護や安定稼働に貢献することができる。また、データ解析プラットフォームである「Splunk」等との連携も検討している。

「PassiveTotalにはAPIのさらなる充実や他サービスとの連携強化を期待したいですね」（小笠原氏）

macnica networks
マクニカネットワークス株式会社
本　　社　〒222-8562 横浜市港北区新横浜1-5-5
TEL.045-476-2010　FAX.045-476-2060
西日本営業所　〒530-0005 大阪市北区中之島2-3-33 大阪三井物産ビル14階
TEL.06-6227-6916　FAX.06-6227-6917