株式会社ミクシィ 様
マクニカネットワークスが提供する スレットハンティングサービスを導入

高度な攻撃グループの侵害痕跡を定期的に調査し、インシデント発生時はアナリストによる調査により適切な対処が可能に

導入のPoint

- 特定の攻撃グループが、内部ネットワークに侵入していないことを定期的に調査
- アンチウイルスやEDRにも反応しなかった潜伏中の不審なファイルを発見し、振る舞いを起こす前に脅威を排除
- マルウェア解析に特化した人材がいない中で、アナリストに相談できる環境を構築でき、迅速な状況判断、適切な対処が可能に

ゲーム業界を狙う攻撃へ対処するため自社に最適なサービスを検討

SNS「mixi」、スマホゲームアプリ「モンスターストライク」の運営会社として知られるミクシィ。「近しい人間関係における豊かなコミュニケーション体験を創出すること」を目指し事業活動を展開している同社では、これまで積み重ねてきた知見や組織力を活かし、スポーツやウェルネスなどの分野でも、コミュニケーションを軸に新たな事業展開に取り組んでいる。

近年標的型攻撃の手口が巧妙化し、特定の会社をターゲットにした標的型攻撃も目立つようになっている。この状況に対応するため、同社ではさまざまなセキュリティ対策について検討を行ったが、中でもスレットハンティングという手法に着目した。はたらく環境室　阿部翔氏は「当社では、多くのユーザーを対象にしたサービスを提供している企業の責任として、これまでもアンチウイルスやEDRなどの製品を導入し、積極的にセキュリティ対策を強化してきました。しかしここにきて攻撃を受ける可能性がさらに高まってきたことから、現在の体制で本当に特定の会社を狙う脅威からシステムを防御できているのか、セカンドオピニオン的な視点から評価したいと考えたのです」と語る。

昨今はゼロデイ攻撃や亜種ウイルスが急増しており、アンチウイルスによる100%の検知は不可能といってよい。一方、EDRにも検知機能は付いているが、ミクシィでの主な用途は何かインシデントが発生した際の検知とフォレンジック（ログ収集）だ。それゆえ同社でも、脅威が社内に潜んでいないかという疑念があったという。開発本部 セキュリティ技術グループ マネージャーの亀山直生氏は「アンチウイルスやEDRはそれぞれ役割が異なりますし、得意分野があります。そこで、これらの対策を補完する意味でスレットハンティングサービスを導入し、潜伏中の脅威がないという確証を得ることにしたのです」と語る。

技術と脅威インテリジェンスに裏打ちされたサービス水準の高さを実感 専門家とのコミュニケーションで安心を得る

スレットハンティングサービスの導入を検討する中で、ミクシィはパートナーから「Mpression Cyber Security Service™スレットハンティングサービス」の紹介を受けた。検討の結果、アンチウイルスやEDR等の既存の対策で防御しきれない脅威を捉えることができる点、特定の攻撃グループの調査（ハンティング）が可能な点、さらに、リモートでメモリを対象としたフォレンジックを実施できる点などが高い評価を受けた。

「EDRはメモリのダンプなどの情報までは取得できますが、その解析となるとフォレンジックベンダーへ

User Profile

株式会社ミクシィ

名　　称：株式会社ミクシィ
所 在 地：東京都渋谷区東1-2-20 住友不動産渋谷ファーストタワー 7F
導入時期：2019年3月
U R L：https://mixi.co.jp

1997年11月に求人情報サイト「Find Job!」の運営を開始。2004 年には日本におけるソーシャル・ネットワーキング サービス（SNS）の草分けである「mixi」の運営をスタートさせ、2006年には社名も株式会社ミクシィに変更した。ゲーム分野では、2013年にリリースしたスマホゲームアプリ「モンスターストライク」が大ヒット。現在も「ユーザーサプライズファースト」を企業理念に、コミュニケーションサービスを通じて顧客に想像や期待を超える価値を提供していくことを目指している。

開発本部
セキュリティ技術グループ
マネージャー
亀山 直生 氏

はたらく環境室
阿部 翔 氏

はたらく環境室
小泉 孝能 氏

「スレットハンティングサービス」導入事例

株式会社ミクシィ 様

の依頼が必要になってしまいますし、高額のコストがかかります。その点、スレットハンティングサービスではわざわざこちらで動かなくても、マクニカネットワークスが持つインテリジェンスを通じて解析してくれる点が魅力でしたね」（亀山氏）

また、本サービスには、ゲーム業界に精通し、長年アジア圏で活動するサイバー攻撃者を分析してきたTEAM T5社の技術と脅威インテリジェンスが投入されている。はたらく環境課の小泉孝能氏は「マクニカネットワークスがTEAM T5との連携をとってくれたおかげで、彼らと情報交換でき攻撃グループの特徴が理解できました。おかげで攻撃を仕掛けてくる相手の姿が見えてきたのは大きかったですね」と語る。

中国圏で感染が多くみられる、潜伏中の不審なファイルを発見 特定の攻撃グループがPC内に潜伏していないことを確認

採用を決定した後、導入工程について阿部氏は次のように語る。「エージェントの常駐が不要で、軽量なスキャナーをグループポリシーに基づいて配布することができるため、導入は容易でした。一部の部署でテストしたのち1週間程度で1500台の社内PCに展開しましたが、特にトラブルは起きていません。もちろん、ユーザーは何も意識していないと思います」

サービスの導入後、さっそく社内に不審なファイルが発見された。この不審なファイルは、アンチウイルスの網を抜けて侵入していたが、その時点では何の振舞いもしていなかったため、EDRからも検知されなかったという。

「潜伏段階で不審なファイルをいち早く検出し、危険な振る舞いを行う前に押さえられたのは大きな成果だと考えています。あらためて、スレットハンティングサービスの質の高さを感じました。また今回のサービスの導入により、標的型攻撃に強いインテリジェンスを持ったセキュリティアナリストが調査した結果、特定の攻撃グループがPCに潜伏していないことを確認することができ、今後も継続的に調査できる点も安心感につながっています」（亀山氏）

アナリストに相談できる環境が出来たため、迅速な状況判断、適切な対処が可能に

ハンティングツールから検知アラートが上がってきたときに、アナリストに相談できるようになったことは、自社にマルウェア解析に特化したアナリストがいないミクシィでは非常に助かっているという。

「現状だとマルウェアの配備に気づくタイミングは色々ありますが、マルウェア本体を駆除するだけで良いのか不明なケースがありました。ハンティングサービスではメモリやレジストリなど端末に残った痕跡からどのような対処が必要か分析し、レポーティングしてくれるため、同じマルウェアの再配備防止など含め適切な対処が可能になりました。自社にマルウェアのアナリストがいなくても、マクニカネットワークスがアナリストの役割を果たしてくれているため、まだ潜伏段階のマルウェアに対しても納得感を持って対処できるのはありがたいです。また攻撃や不審なファイルを発見した時にすぐ調査できることや、年間利用契約なので回数による費用の増加を気にせず気軽に利用できるのは魅力です。サポート対象に含まれるWindows端末については全台に対し調査を実施していますが、同じ台数と回数の調査をフォレンジックベンダーに依頼すると、現状だとかなりの費用と時間がかかると思います」（亀山氏）

システム導入して終わりではなく、一緒に汗をかいてくれるマクニカネットワークスへの期待

ミクシィでは、Macを除いた1500台の社内PCに対して週1回調査を実施。感染の有無を調査しているが、現時点では脅威が存在していないことを確認できている。亀山氏は「システムは導入して終わりではなく、運用まで実施できて初めて効果があります。マクニカネットワークスはハンティング調査や解析を通して一緒に汗をかいてくれることに安心感があります。また、メモリ解析をしてくれる製品は当社では新しいため、システム連携を行うことでセキュリティ監視の自動化や改善にも役立てていきたいと考えています。マクニカネットワークスはマニアックな情報を持っていて、最新のものをいち早く提供してくれるので、これからもセキュリティの相談役としてとても期待しています」と語ってくれた。

https://www.macnica.co.jp/

MACNICA

mPRESSION Cyber Security Service

マクニカグループの各事業会社で開発するオリジナル技術ブランド「Mpression（エムプレッション）」の中で、サイバーセキュリティに関するソリューションのブランドです。

株式会社マクニカ　ネットワークス カンパニー
〒222-8563 横浜市港北区新横浜 1-5-5
TEL.045-476-2010　FAX.045-476-2060
西日本オフィス
〒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
sec-service@macnica.co.jp

© Macnica, Inc.
● 本カタログに掲載の製品仕様は、予告なく変更する場合があります。予めご了承ください。
● 本カタログに掲載されております社名および製品名は、各社の商標及び登録商標です。