



# ExtraHop

## 壊滅的になる前にランサムウェアを阻止!

ExtraHopは、IT部門が多くのタイプのランサムウェア攻撃を数分で検出、調査、軽減するための簡単な方法を提供します。環境全体に対するこうしたリアルタイム検出は、これまでは不可能でした。

### ● ランサムウェア向け、独自のExtraHopソリューション!

**他製品では、全てのNASシステム、ファイル共有、または共有ドライブにわたるランサムウェアのアクティビティを検出することができません。**

- ExtraHopは、ランサムウェア攻撃がネットワーク上で観測されてから数分以内にIT部門に通知します。
- ITチームは、ランサムウェアを検出するだけでなく、誰が悪意のあるファイルを受信したか、マルウェアをホストしているIPアドレスについて確認・検索することもできます。
- 攻撃を数分以内に検出・阻止することによって、組織は運用の混乱や金銭上の損失を防止することができます。

### ● 知っていましたか?

- IBMの調査によると、ランサムウェアに感染した企業の70パーセントが身代金を支払いました。
- FBIの推定では、2016年にはランサムウェアは10億ドル以上を犯罪者にもたらしました。
- シマンテック(Symantec)によると、2016年の平均身代金要求額は、2015年末時点での要求額の2倍以上である679ドルでした。
- ランサムウェアは、Malwarebytesアンチウイルスソフトウェアが遭遇したマルウェア感染の約60パーセントを占めています。

詳細については、以下のホワイトペーパーをダウンロードしてください。

<https://www.extrahop.com/platform/resources/whitepapers/ransomware-detection-and-prevention/>  
(新しい軽減アプローチを用いたランサムウェアの検出と阻止)

ランサムウェアは、ハッカーが金儲けするための低リスク・高報酬の方法として始まりました。ハッカーはますます企業を標的としています。ExtraHopは伝送中の全てのデータを解析するので、IT組織は完全なネットワーク可視性が得られます。ExtraHopプラットフォームにより、インシデント対応チームは数分以内に攻撃について把握し、影響を軽減するための迅速な対策を講じることができます。

### ● 検出 - 環境内部で脅威をより迅速に検出

ExtraHopプラットフォームは、ランサムウェアに関連する独自のストレージWRITE動作やファイル変更を含む、ネットワーク上の異常を検出します。インシデント対応チームは、アラートを設定し、数分以内にランサムウェア感染の通知を受けることができます。

### ● 調査 - すべての感染したマシンと悪意のあるIPを突き止める

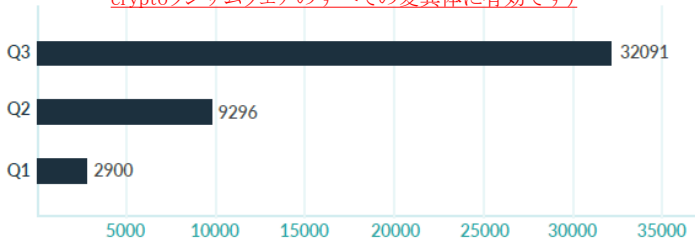
ランサムウェアがファイルを上書きするにはある程度の時間を要するので、インシデント対応チームが数分以内に攻撃を突き止められることが非常に重要になります。ExtraHopプラットフォームにより、チームは、NASシステムや共有ファイルインフラ上で進行中の攻撃を迅速に特定することができます。又、対応チームは、悪意のあるファイルを受信したユーザやマルウェアをホストしているIPアドレスを迅速に特定することができます。

### ● 阻止 - ファイアウォールやネットワークアクセス制御と統合する

ExtraHopが提供する特定のデータを用いることで、インシデント対応チームは、感染したコンピュータとの接続を解除し、悪意のあるIPアドレスをブロックし、バックアップからのファイル復旧を開始することができます。

- カスペルスキー(Kaspersky Labs)によれば、新しい'cryptor'の変種の数、2016年のQ2からQ3に3倍以上増加しました(下表)。

(ExtraHopは、挙動を観測することによってランサムウェアを検出するので、cryptoランサムウェアのすべての変異体に有効です)



● **ExtraHopを用いたランサムウェア検出**

ExtraHopプラットフォームは、伝送中の全てのデータ(全てのクライアント、ネットワーク、アプリケーション、インフラのアクティビティ)を解析して、リアルタイムのセキュリティの見識からなる豊富な情報源を提供します。

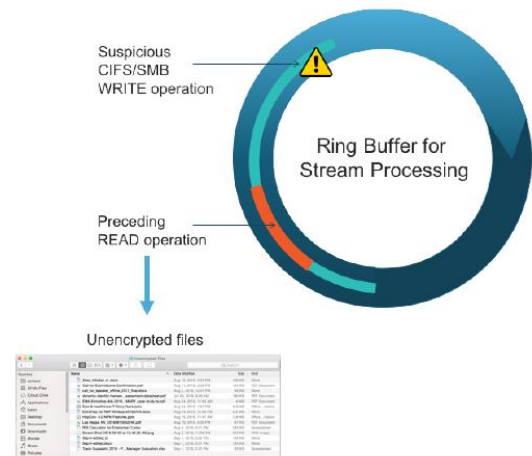
ランサムウェアを検出するためのExtraHopソリューションは、例えば、不正な形式のファイル拡張子を使用している疑わしいCIFS/SMB WRITE動作を特定します。

Cryptowallなどのランサムウェアの変異体は、ファイルが暗号化されるときにファイル名や拡張子を変更して、例えば「asksdf.ui4」や「sdfdferr.u8i3」となるようにします。

ExtraHopプラットフォームは、検出以外にも優れた調査機能を提供します。容易にドリルダウンして、どのクライアントが悪意のあるファイルを受信したか、どのIPアドレスからマルウェアがダウンロードされたかを確認することができます。

このプラットフォームにより、ファイアウォールやネットワークアクセス制御のアクションを自動化することが可能になるので、通信のブロックや感染したマシンの隔離を行うことができます。

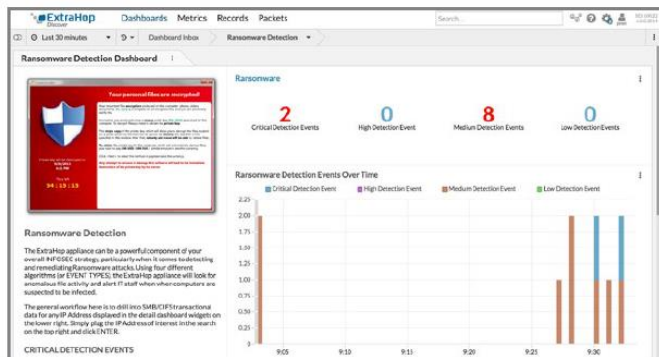
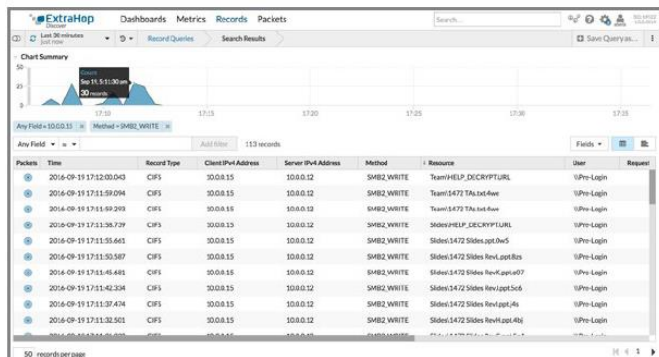
READ動作のみのパケットキャプチャからファイルを再構築することもできます(右側の図を参照)。



**WireDataでバックアップ!**

ExtraHopは、疑わしいWRITE動作に先行するREAD動作のパケットを正確にキャプチャすることができるので、暗号化されていないファイルを再構築することができます。

以下の画面は、数台のサンドボックス型ワークステーションを通じて伝搬するCryptowallの感染を示したものです。このソリューションは、ExtraHopの顧客の環境内でのランサムウェアの検出にも成功しました。

Time	Record Type	Client IP Address	Server IP Address	Method	Message	User	Request
2016-09-15 17:12:00.043	CIFS	20.88.15	10.8.0.12	SMB2_WRITE	TeamHELP_DECRYPTUREL	10PheLapp	
2016-09-15 17:11:59.094	CIFS	20.88.15	10.8.0.12	SMB2_WRITE	Team1477_Thead-fee	10PheLapp	
2016-09-15 17:11:49.293	CIFS	20.88.15	10.8.0.12	SMB2_WRITE	Team1477_Thead-fee	10PheLapp	
2016-09-15 17:11:36.739	CIFS	20.88.15	10.8.0.12	SMB2_WRITE	TeamHELP_DECRYPTUREL	10PheLapp	
2016-09-15 17:11:35.641	CIFS	20.88.15	10.8.0.12	SMB2_WRITE	Sides1472_Sides_Rev1.appl-0u5	10PheLapp	
2016-09-15 17:11:35.587	CIFS	20.88.15	10.8.0.12	SMB2_WRITE	Sides1472_Sides_Rev1.appl-0u5	10PheLapp	
2016-09-15 17:11:45.481	CIFS	20.88.15	10.8.0.12	SMB2_WRITE	Sides1472_Sides_Rev1.appl-007	10PheLapp	
2016-09-15 17:11:42.334	CIFS	20.88.15	10.8.0.12	SMB2_WRITE	Sides1472_Sides_Rev1.appl-5c4	10PheLapp	
2016-09-15 17:11:37.474	CIFS	20.88.15	10.8.0.12	SMB2_WRITE	Sides1472_Sides_Rev1.appl-4b6	10PheLapp	
2016-09-15 17:11:36.261	CIFS	20.88.15	10.8.0.12	SMB2_WRITE	Sides1472_Sides_Rev1.appl-4b6	10PheLapp	

ExtraHopランサムウェア・ソリューションには、疑わしいCIFS/SMBファイル・アクティビティの一つのハイレベル・ビュー用に2つのダッシュボードがあります。

そのダッシュボードから、トランザクション・レコードを容易に調査して、感染の範囲と発生源を把握することができます。

● **オンラインデモをご体験いただけます!**

オンラインデモでは、セキュリティの使用事例でExtraHopプラットフォームが行える内容をご覧いただけます。ご自身でインターフェースをご検証いただけるほか、ランサムウェア検出や脅威検出などのガイドツアーにご参加いただけます。

[www.extrahop.com/demo](http://www.extrahop.com/demo)



**ExtraHop Networks社について**

ExtraHop Networks社(アメリカ、シアトル)は、リアルタイムのワイヤデータ解析におけるグローバルリーダーで、ITをよりアジャイルかつプロアクティブにするのに必要なリアルタイムのオペレーション・インテリジェンスを提供します。アドビ(Adobe)、アラスカ航空(Alaska Airlines)、コンカー(Concur)、エクスペディア(Expedia)、マイクロソフト(Microsoft)を始めとする世界で最も成功しているIT組織は、ExtraHopを使用して50万台以上のデバイスを管理し、毎日1兆を超えるトランザクションをモニターしています。