２０１７年　５月１５日

お客様各位

株式会社日立ソリューションズ
Palo Alto Networks 製品ユーザーサポート

ランサムウェア WanaCrypt0r の対応について

拝啓　平素は Palo Alto Networks 製品ユーザーサポートをご利用頂きまして誠にありがとうございます。
ランサムウェア WanaCrypt0r からお客様システムを守る方法について、Palo Alto Networks 社から以下のアナウンスが出ています。
ランサムウェアの感染を防ぐため、以下対策の実施をご検討下さい。

敬具

記

1. Palo Alto Networks 社アナウンス
   http://researchcenter.paloaltonetworks.com/2017/05/palo-alto-networks-protections-wanacrypt0r-attacks/

2. 日本語訳

   Palo Alto Networks WanaCrypt0r ランサムウェア攻撃に対するプロテクション

   何が起こったか：
   2017 年 5 月 12 日金曜日、WanaCrypt0r の最新亜種による一連の攻撃が広範囲に対して始まりました。これらの攻撃は世界中の公的・民間組織に影響を与えたと報告されています。Palo Alto Networks の次世代セキュリティプラットフォームはこの攻撃に対するプロテクションを自動で作成、配布、適用を行いました。

   どうやって攻撃されるのか：
   WanaCrypt0r はリンクもしくは PDF ドキュメントを添付したフィッシングメールによる攻撃が始まります。フィッシング攻撃の成功により WanaCrypt0r ランサムウェアはターゲットシステムに感染し、次に SMB プロトコル経由で Microsoft Windows システムにある EternalBlue 脆弱性（CVE-2017-0144)を悪用して広範囲に感染を広めようとして攻撃します。この脆弱性は Microsoft により MS17-010 <https://technet.microsoft.com/en-us/library/security/ms17-010.aspx> として 2017 年 3 月に対応されています。この脆弱性は Shadow Brokers グループによって 2017 年 4 月に一般公開されていました。MS17-010 のパッチを適用している組織は WanaCrypt0r の感染がネットワークを介して広まるリスクはありません。MS17-010 は現在アクティブな攻撃で使用されているネットワークコン

ポーネントにあるリモートコード実行可能な脆弱性を修正しているため、私たちはこのセキュリティアップデートの適用を早急に行うことを強くおすすめします。

阻止：
Palo Alto Networks のお客様は、攻撃ライフサイクルのいずれにおいても脅威を自動的に止めることができる脅威阻止アプローチを適用している我々の次世代セキュリティプラットフォーム経由で守られています。Palo Alto Networks のお客様は次世代セキュリティプラットフォームに対して提供している複数の脅威阻止コントロールを通じて自動的に WanaCrypt0r ランサムウェアから守られています。

WildFire はすべての既知サンプルをマルウェアとして分類し、悪意のあるコンテンツがユーザに配布されることを自動的にブロックしています。

Threat Prevention はこの攻撃に使用されている脆弱性の悪用(CVE-2017-0144 - MS17-010)に対応する IPS シグネチャを適用しています。

Traps はエンドポイントで WanaCrypt0r マルウェアの実行を阻止します。

AutoFocus は WanaCrypt0r タグ <https://autofocus.paloaltonetworks.com/#/tag/Unit42.WanaCrypt0r> を通じて脅威分析と脅威ハンティングできるようこの攻撃を追跡します。

GlobalProtect を通じて次世代ファイアウォールポリシーをモバイルユーザに拡大することでリモートワーカーを守ることができます。

Palo Alto Networks 次世代セキュリティプラットフォームを使ってランサムウェアを阻止するベストプラクティスについてはこちらのナレッジベース <https://live.paloaltonetworks.com/t5/Featured-Articles/Best-Practices-for-Ransomware-Prevention/ta-p/74148> を参照ください。

3. ランサムウェア WanaCrypt0r 攻撃に対するプロテクションの対応シグネチャバージョン

（CVE ID 2017-0143 ～ 2017-0148）

Last Update	First Release	CVE ID	Threat ID	Severity	Action	Attack Name
695-4002 2017/05/02 UTC	695-4002 2017/05/02 UTC	CVE-2017-0148	32716	critical	reset-server	Microsoft Windows SMB Remote Code Execution Vulnerability
692-3988 2017/04/27 UTC	692-3988 2017/04/27 UTC	CVE-2017-0146 CVE-2017-0147	32427	critical	alert	Microsoft Windows SMB Remote Code Execution Vulnerability
692-3988 2017/04/27 UTC	688-3964 2017/04/19 UTC	CVE-2017-0145	32424	critical	alert	Microsoft Windows SMB Remote Code Execution Vulnerability
698-4026 2017/05/13 UTC	688-3964 2017/04/19 UTC	CVE-2017-0144 CVE-2017-0146	32422	critical	reset-both	Microsoft Windows SMB Remote Code Execution Vulnerability
696-4015 2017/05/09 UTC	696-4015 2017/05/09 UTC	CVE-2017-0143	32494	critical	alert	Microsoft Windows SMB Remote Code Execution Vulnerability
692-3988 2017/04/27 UTC	688-3964 2017/04/19 UTC	CVE-2017-0143	32393	critical	alert	Microsoft Windows SMB Remote Code Execution Vulnerability

※シグネチャバージョン 698-4026 で、Threat ID 32422 が更新されています。
2017/05/15 時点では、ランサムウェア WanaCrypt0r 攻撃に対するプロテクションの対応 シグネチャバージョンとして、バージョン 698-4026 以降のご利用をご検討ください。

以上