サプライチェーン攻撃の実例

セキュリティスイッチの有効性

SubGate
https：//www.subgate.co.jp


K拡散制作所
みんなも知っての通り、


我が社は長年親会社の、
サプライチェーンの中核を担ってきた
拡散製作所・社長
雨宮 豪


しかし昨今、そのサプライチェーンを狙った
サイバー攻撃が激化している


これだけ警鐘が鳴らされている最中に感染事故を起こしたら
信頼失墜だ！


それを防ぐ最善の手段はこれまでと同じです
不審なメールは
絶対×100に開かないでください！
下請けにも徹底するように伝えてください！
はい！


緩過梱包会社
（下請け）
最近変なメール増えてないか？
絶対開かないでくださいよ
元請けにめっちゃ厳しく言われてるんですから
え～、そうなの？
オレ、ちょいちょい開いちゃってるけど～？
なんかオレ宛てとしか思えない件名で来るからさ～…
カタ
カタ
は…？
うそ…ええ
せ…先輩の使ってるパソコンが

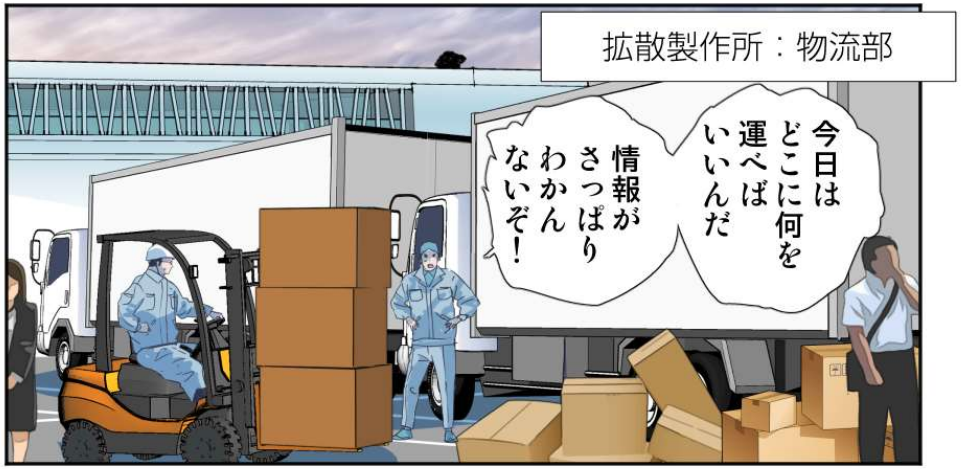

ウイルスに感染してるんじゃないすか……
だから最近変なメールが多いんだ…
ウイルス!?
先輩、絶対元請けのパソコンも感染させましたよ…
もし、元請けの親会社まで感染させてたら…
オレら…終わりっすよ…


拡散製作所
あ、親会社のシステム部から電話だ
お疲れ様ですどうされましたか？
ブーブーブーブー
親会社
どうもこうもないよ！
おたくからサイバー攻撃を受けている痕跡があるんだ！
大至急調査して報告しろ！
結果によってはただじゃ済まないぞ！
も…も…


申し訳ございません！
すぐに原因を調査いたします
拡散製作所：システム部
どういう事なんだ！
システムがダウンしているぞ！
ランサムウェアに感染しています！
何だって？
拡散製作所：営業部
申し訳ありません！親会社の佐藤さま
実は弊社のシステムがダウンしてしまい…
ですが今日納品の物品だけは必ず、お届けします！


拡散製作所：経理部
大変申し訳ございません…
実は…弊社のシステムがダウンしてしまい…
御社の支払先口座から教えて頂けますか…


拡散製作所：人事部
えー！
あのシステムが落ちたのでお給料は
現金支給になります…


拡散製作所：物流部
今日はどこに何を運べばいいんだ
情報がさっぱりわかんないぞ！


この日、拡散製作所は出荷もできず…
親会社の生産ラインを完全に止めてしまった…
おおっ


社長…感染ルートが判明しました
最初にウイルスに感染したのは…
下請けの会社のパソコンでした
下請けだと!?


もおおしわけエエ
ございませんでしたあああ！


うっかり開いてはいけないメールを、
開いてしまいました…！


こ…高額な、ペナルティだけじゃない…


最悪の場合…
取引停止になってしまうんだぞ…


だからあれほど…下請けでも
注意するように言ったじゃないかああ…！
ホッ


社長…、
こうなった以上、


サイバーセキュリティの専門家に相談しませんか


拡散制作所
サイバーセキュリティの専門家？

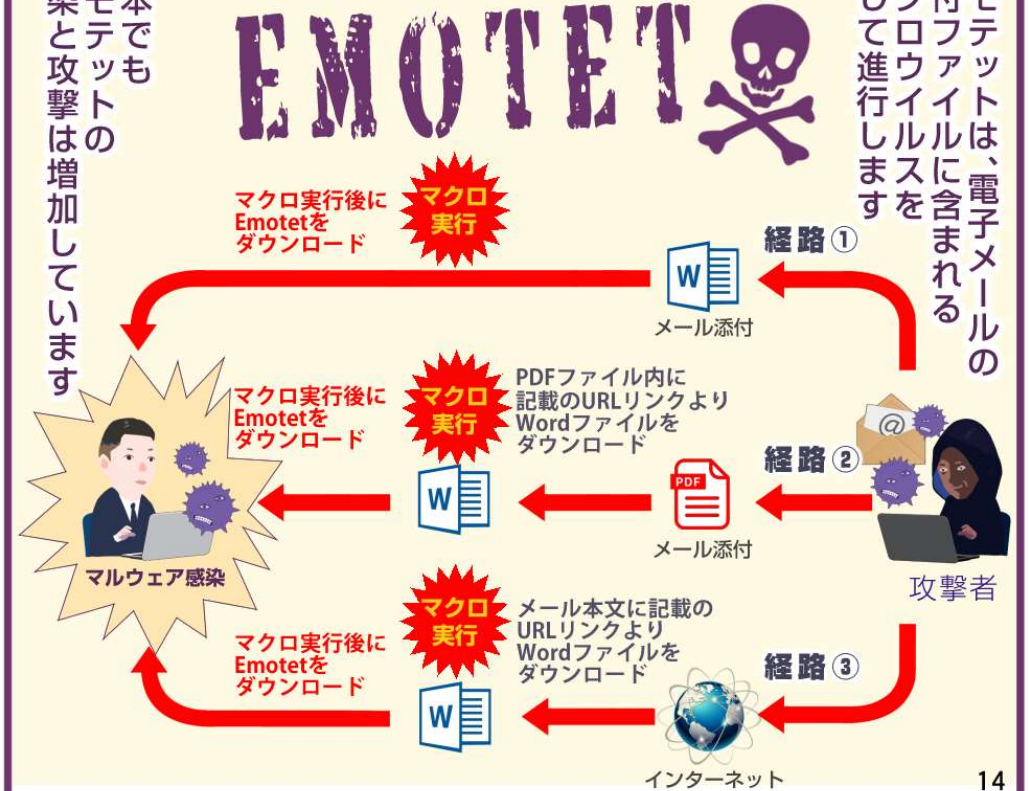

話は伺いました、
風間 守です


早速ですが、こちらで原因を突き止めましたところ、
もう突き止めたのか


型番: XYZ AB12 Ver:1.0
S/N: 123A4560987
MAC:AA-32-C4-BA-DA-12
ワイヤレス パスワード/PIN:123456789
SSID: PassWord_ABC_123
SSID: PassWord_ABC_123_5G
下請けのルーターのパスワードが、デフォルトのままでした

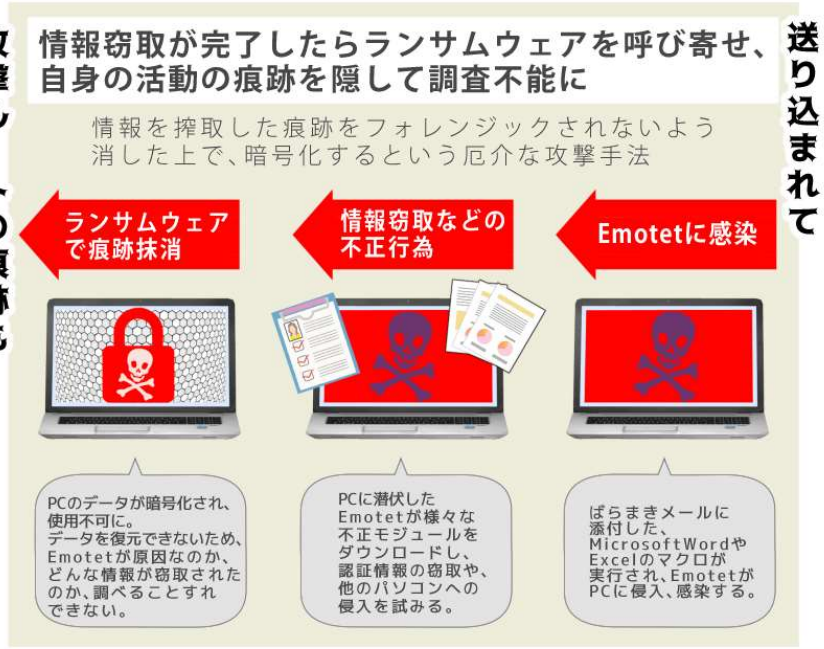
エモテットは、電子メールの添付ファイルに含まれるマクロウイルスを介して進行します

日本でもエモテットの感染と攻撃は増加しています



最終的にエモテットのプラットホームからランサムウェアを送り込まれて

攻撃ルートの痕跡も全て暗号化されてしまいました



セキュリティスイッチ？

これは感染することを前提に

対策をとるシステムです

感染を…前提に!?

メール等から感染する前提で、拡散防止を講じるってことですか

そうです

ウイルスの脅威は年々増し、もはや感染を完全には防ぎきることは困難です

このセキュリティスイッチは感染した端末からの

次のデバイスへの拡散を防止できるHUBです

脅威を検知しました。

有害なパケットを出しているパソコンを特定する上に、

それを通報してくれるのか！

緊急警報

RANSOM PANDEMIC

そのメールを開いてはならない