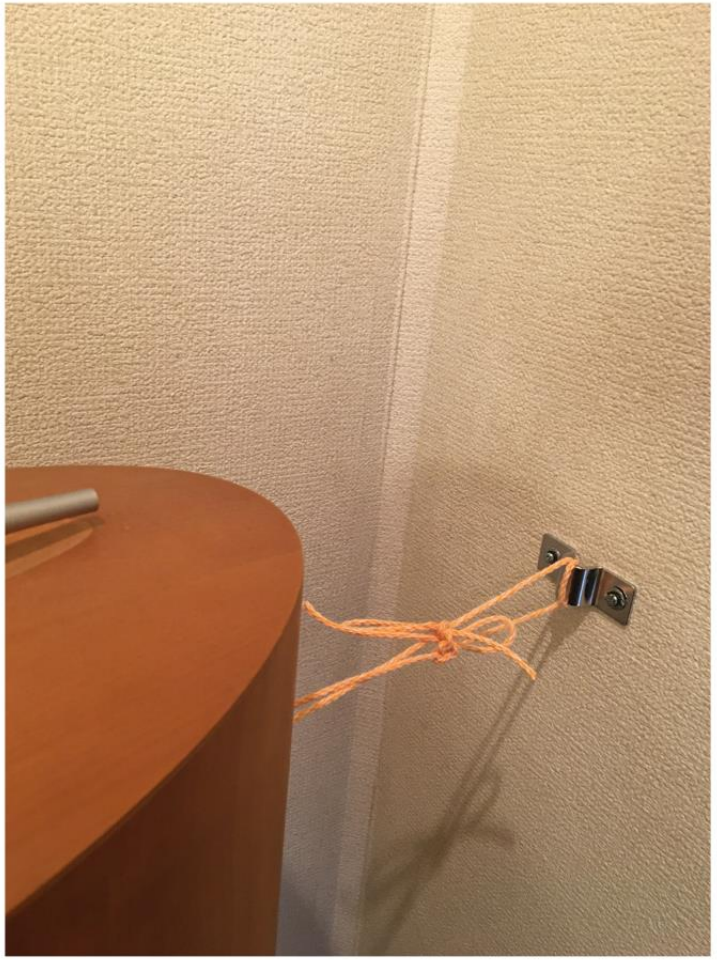
災害に備える

株式会社　ムービット

地震に備える



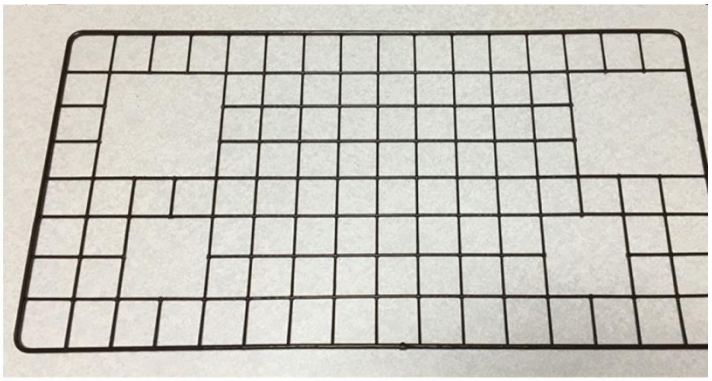
地震に備える

石膏ボート用　　（ボードアンカー）

地震に備える

コンクリート用　　（プラグ）

地震に備える



身代金要求　ランサムウエア による　災害

ダークWeb / データやアクセス権の売買

■「ランサムウエア」月120ドルから

真相深層

サイバー攻撃 闇市場拡大

サイバー攻撃ツールの闇市場が拡大している。身代金目的で端末内のデータを暗号化するランサムウエア、標的となる組織に不正アクセスできる権利などが売り出され、競争が新たな商品を生み出していく。技術がなくても「武器」の調達が可能になり、攻撃者の裾野拡大が懸念されている。

「最も安い検出不能ランサムウエア」。1カ月で120ドル、6カ月で490ドル、12カ月で900ドル――。

サブスク利用も

キャノンマーケティングジャパンが確認したランサムウエアの販売サイトでは、サブスクリプション（定額課金）の利用プランが設けられ、最も高額なプランでは感染を容易にする追加機能も付くとされていた。

ランサムウエアは今年だけで既に3回バージョンアップされ、使い方は「よくある質問」に答える形で説明。検出を免れるウイルス対策ソフトの一覧も載せていた。

同社の西浦真一セキュリティエバンジェリストは「セールスポイントや使い方を丁寧に説明する様は一般的なソフトウエアやアプリの販売サイトと変わらない」と話す。

匿名性の高い闇サイト群「ダークウェブ」ではこれまで、流出したクレジットカード情報やSNS（交流サイト）アカウントが流通しており、近年、取引の対象は一段と多様化している。

トレンドマイクロによると「日本の医療系大学のネットワークに侵入するアクセス権」は999ドル、ATMから銀行のネットワークに侵入するマルウエア（悪意のあるプログラム）は2千ドルで売り出されていた。偽サイトへの誘導などに使うショートメッセージサービス（SMS）の配信を5千件350ドルで請け負うとの書き込みもあった。

販売が確認されたサイバー攻撃用のサービスやツール

医療系大学へのアクセス権	999ドル
米有力企業へのアクセス権	1万ドル
ATM用のマルウエア	2000ドル～
ランサムウエアのサービス	年間900ドル
スパムSMSの送信サービス	25～500ドル
SMS送信用のソフトウエア	499ドル～

（出所）トレンドマイクロ

売り手で競争、脅威増す

キャノンマーケティングジャパンが確認したランサムウエアの販売サイト＝同社提供

セキュリティー関係者によると、国内38社などから漏洩した疑いが明らかになったVPN（仮想私設網）の利用情報は、有料の会員制サイト内でやり取りされていた。

サイバー攻撃をサポートするマルウエア販売や代行サービスは「CaaS（クライム・アズ・サービス）」とも呼ばれる。CaaSを利用することで「高度な技術や専門知識がなくても攻撃を実行できるようになっている」と、トレンドマイクロの岡本勝之セキュリティエバンジェリストは警鐘を鳴らす。

売り手としては、自ら標的を探して攻撃を仕掛けなくても、得意分野の技術を生かして効率的に稼げるメリットがある。マルウエアを提供し、攻撃で得た収益の一定割合を成功報酬として受け取るケースもある。

機能の劣るマルウエアは市場で淘汰され、攻撃が成功しやすいほど価格は上がる。

ロシアのウイルス対策ソフト開発会社「ドクターウェブ」のボリス・シャロフ最高経営責任者（CEO）は「売り手が競い合うことでマルウエアなどの攻撃力が高まる構図になっている」と指摘する。ランサムウエアで暗号化されたデータの復旧サービスでも「数年前と比べ、データを復元できないケースが増えている」（柏木渡真）

歯止め難しく

マルウエアの販売は国内では不正指令電磁的記録提供の罪にあたる。ただ「不正なプログラムといえるかどうかは実際に使用されて初めて検証できる」と警察関係者は説明する。被害が発生した場合は攻撃の実行者の検挙が優先されるため「マルウエアの提供者を追及し、闇市場の取引に歯止めをかけるのは難しい」という。

海外ではおとり捜査で闇市場サイトを閉鎖に追い込んだ事例もあるが「日本では捜査権限が限られる」とセキュリティー会社スプラウトの高野聖玄社長は指摘する。「サイバー攻撃や闇市場に国境はない。国際的な捜査連携や捜査手法の見直しによって抑止力を高めていくことが必要だ」と話している。（柏木渡真）

医科系大学へのアクセス権
　999ドル

米国有力企業へのアクセス権
　1万ドル

ランサムウエアのサービス
　900ドル

2020/9/5 日本経済新聞

ダークWeb / カプコン

カプコン

ランサムウエアで被害か

サーバーのデータを暗号化された

一部のデータをダークWebへ公開

１１億円の金銭要求

2020/11/12 Yahoo News

米国石油パイプライン　コロニアル

ハッカー集団　「ダークサイド」 によるランサムウエアで被害

東海岸の45%が一本のパイプラインに依存（全長　8850Km ）

5億円の支払い

操業停止期間
　5月8-13日

米東海岸の45%の石油を支えるパイプライン


米パイプラインサイバー攻撃
身代金の大半奪還
司法省

2021/06/08 日経

2021/5/17

ニップン　　2021・7・7

国内の製粉大手がサイバー攻撃の被害に、ランサムウェア対策にはオフラインバックアップが有効

DLIS・柳谷 智宣　2021年9月3日 06:00

ツイート　リスト　B! 23　Pocket 25　いいね！ 28　シェア

2021年7月7日、株式会社ニップンはグループ企業で利用している複数のシステムで障害が起きていることに気が付きました。すぐにネットワークを遮断して、外部のセキュリティ専門家に調査を依頼したところ、サイバー攻撃を受けたことが判明しました。

同時多発的にサーバーや端末のデータを暗号化されてしまったのです。財務管理や販売管理を行う基幹システムに加え、グループネットワーク内で運用しているシステムも被害に遭いました。

国内の製粉大手のニップンが大規模なサイバー攻撃を受けました

専門家は、システムの起動もできないうえ、バックアップサーバーも同様に暗号化されており、復旧に有効な手段はないと報告しました。今回のような広範囲に影響を及ぼすケースは例がないとのことです。

同社は、BCP（事業継続計画）対策を取っており、データセンターを分散設置していました。しかし、今回は想定していた事態を上回り、多くのサーバーが同時攻撃を受けてしまったのです。

BCP対策としてデータセンタを分散

バックアップサーバーも暗号化された

想定外の規模で対処できなかった

病院　2021・10・14

患者の治療中に
代替システムを使用し
患者の情報を手書き
で書き留めている

ダークサイド / アフリエイト

- アフリエイト　　面接に合格する必要あり
- 合格　　RaaSの管理パネルへのアクセス権

- ダークサイドの取り分　　身代金の10-25%　（仮想通貨）

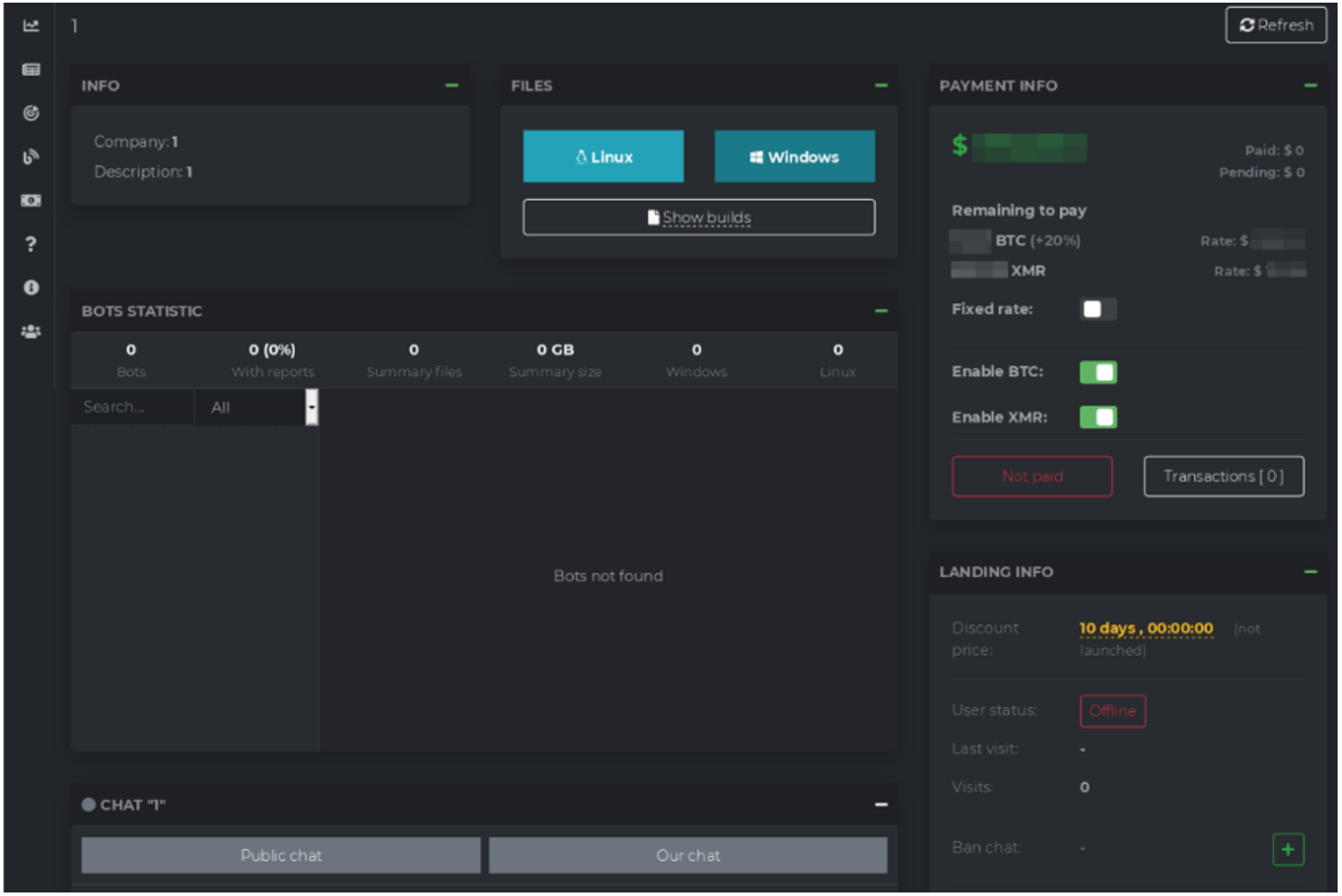
身代金　50万ドル未満　　25%

身代金　500万ドル以上　　10%

（出所：日経クロステック）

ダークサイド / RaaSの管理パネル

RaaS（Ransomware as a Service）



（出所：ファイア・アイ）

ダークサイド / 機能

1）データを盗み出してからランサムウエアで暗号化

2）身代金要求

3）ダークWebでデータの公開

- 2021年3-4月ごろに機能追加

4）身代金の支払いに応じない企業に大量のデータを
送りつけるDDoS攻撃の機能を追加

5）コールセンターから脅迫電話をかける機能
ダークサイドRaaSの管理パネルから
身代金を支払うよう企業に圧力をかける電話を手配

（出所：日経クロステック）

対応策　/　攻撃を防ぐには

１）身代金要求には応じない　（建前）

お金があるなら　払うのもありかも（値引き交渉も）

ただし　暗号化されたファイルが復元できる保証もない

また、攻撃が　一度で終わる　保証もない

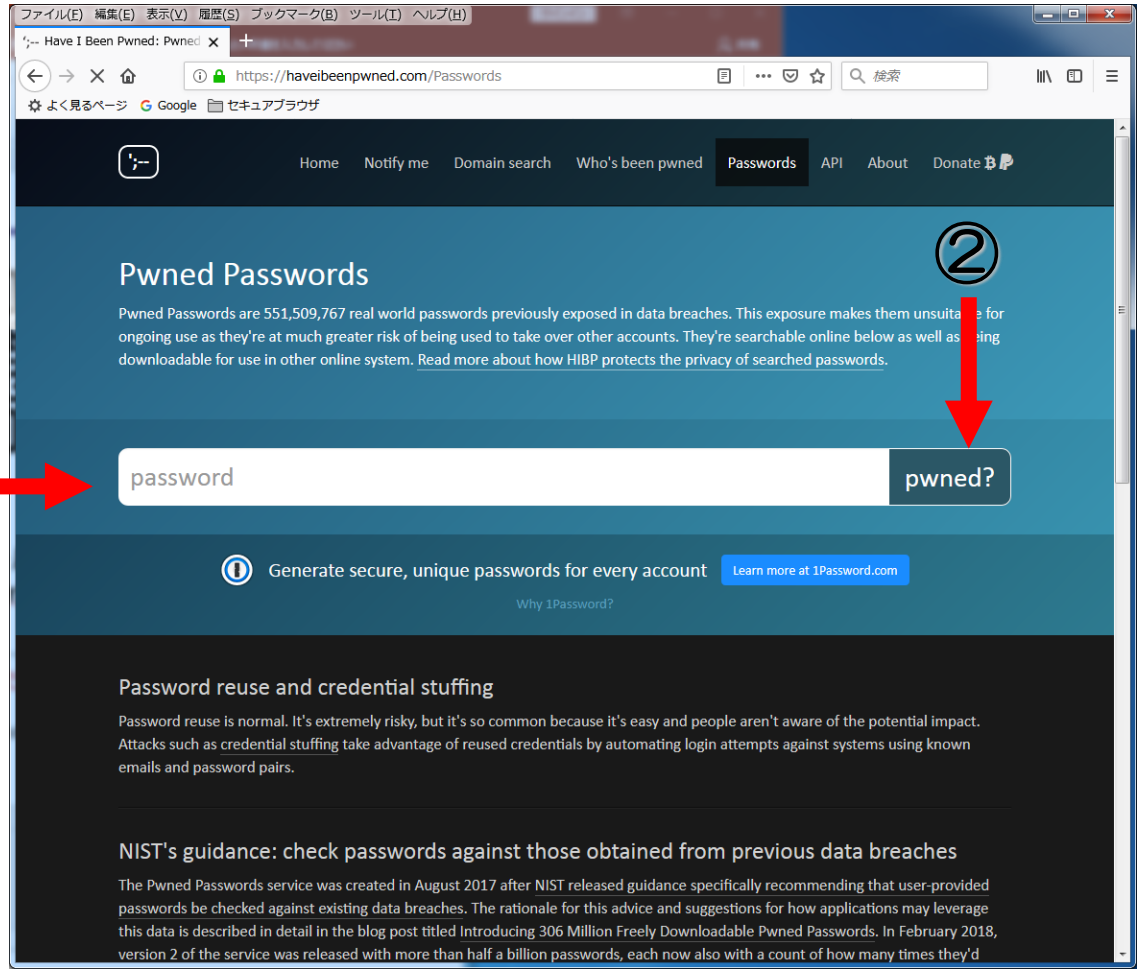
２）サイバー保険　？

保険会社が関連費用の全額を引き受ける保証はないため

３）バックアップ

アカウントやパスワード流出チェックサイト

https://haveibeenpwned.com/



① パスワードを入力
② pwned？　を押す

Oh no --- pwned !
残念でした

Good news — no pwnage found!
大丈夫