FACTA online - 総合情報誌[ザ・ファクタ]

打つ手なし「jpドメイン」攻撃

ネットバンキングなどのDNSに最強の「毒入れ」手法が登場。JPRSの警告はお座なりだ。

2014年6月号

「カミンスキー型攻撃」を公表したダン・カミンスキー氏

AP/Aflo

4月15日、「jp」ドメインを管理する日本レジストリサービス（JPRS）が緊急警報を発した。「キャッシュポイズニング（毒入れ）攻撃の危険性増加に伴うDNSサーバーの設定再確認について」というタイトルで、ネットワーク管理者に対し「毒入れ攻撃」に注意を促す内容と対策が記載されていた。

まず「毒入れ攻撃」とは何か。ネットバンキングで利用しているいつもの銀行サイトが、実は本物そっくりに作られた偽物で、入力したログインIDとパスワードが悪意の第三者の手に渡ってしまう――といったサイバー攻撃を実行する手法のことだ。

この手口だと、見た目だけ真似た偽サイトと異なり、ブラウザー（閲覧ソフト）のアドレス欄に本物のURLを表示させることができ、一般ユーザーが見抜くことはほぼ不可能だ。

ドメイン名と、インターネット上の住所にあたるIPアドレスの照らし合わせを行うDNS（Domain Name System）サーバーに、第三者がこっそり仕掛ける「罠」のようなものをイメージするといい。サーバーの情報をこっそり改竄するので俗に「毒入れ」と呼ばれているが、毒入れされたDNSサーバーは、パソコンからのIPアドレスの問い合わせに対し偽のIPアドレスを返答し、アクセスを偽サイトへ誘導してしまう。

「jp」全方位の機関銃

DNSサーバーは、基本的にプロバイダーやデータセンターなどのネットワーク事業者が管理と運営を行っているので、一般ユーザーは為す術がない。

すべてがネットワーク上で実行されるので、パソコン内のウイルスソフトでスキャンしても検知できない。アクセス先を本物であるかのように偽装することができるので、被害にあったことすら気がつかないユーザーがいる可能性もある。

ネットバンキング偽装だけでなく、企業や政府サイトの偽装・改竄、電子証明の不正取得、任意のメールをインターセプトして改竄するなど、それこそ何でもありの世界なのだ。

DNSの仕組み上の欠陥を突いたものであり、1990年代からたびたび被害が報告されている。ただ、効率のよい攻撃手法とは言えなかった。だが、2008年にセキュリティー研究家のダン・カミンスキー氏が攻撃の成功率を飛躍的に高める「カミンスキー型攻撃」という毒入れ手法を公表したことで事態は一変。それ以前の毒入れが「火縄銃」としたら、カミンスキー型は「機関銃」攻撃を可能にしたと言われている。DNSというインターネットの根幹が、とてつもない危険に曝されていることが判明したのだ。

厄介なのは、DNSが基本的に持つ脆弱性を利用した攻撃手法なので、根本対策は今のところ存在しないという点だ。対処療法的に弾に当たったところを修理するか、弾に当たる確率を下げるしか術はない。

解せないのは、今回JPRSが注意喚起したリリースの内容が、2008年当時にカミンスキー型が公表された際に散々言われた「ポートランダマイズ」という防御策を再確認するものだったこと。何を今さらだ。

JPRSは「未対策のDNSが10％存在する」「最近になって大手プロバイダーにカミンスキー型攻撃手法によると思われるアクセスが増加した」からというのだが、関係者の多くが疑問を持ったほどだ。

やがて理由がわかった。中京大学情報理工学部の鈴木常彦教授と研究者の前野年紀氏が、カミンスキー型攻撃を応用したさらに強力な攻撃手法を発見し、2月15日にJPRSに密かに注意を促していたのだ。

カミンスキーが示した手法は、狙い撃ちした特定のドメイン名に毒入れし、そのサーバーへのアクセスを偽サイトなどへ誘導する手法だが、鈴木・前野方式は最後に「jp」が付くドメイン全てを攻撃対象とするもの。言うなれば、特定の的を狙うだけだった「機関銃」を、四方八方への連射を可能にする「全方位機関銃」に変える威力を秘めた強力な手法なのだ。

この「全方位」攻撃に速効性のある防御方法はない。それが証拠にJPRSは、鈴木・前野型の存在を知らされたにもかかわらず、4月15日に「ポートランダマイズ」という6年前からある衆知の対策を注意喚起するにとどまっている。

このJPRSの隠蔽体質には、疑問の念を抱かざるを得ない。強力な攻撃手法が発見されたのに、内容を公表しないまま、従来型の対策でお茶を濁そうとしているか、効果的な対応策を編み出すまでは、ひたすらダンマリを決め込んで騒ぎが拡大しないようにしているのだろうか。

詳細な説明は控えるが「親子同居、ゾーンのないサブドメイン」というDNS設定の脆弱性を突く今回の新手法への対策は、JPRSが運営するDNSの大改造が必要になるので、一朝一夕ではできないからなのか。

IIJの奇妙な沈黙

実際、この件についてJPRSは鈴木教授に「口止めを強いていた」そうだ。でも、一線級のクラッカーはちょっとしたヒントで突破口を見つけ出す。鈴木教授はJPRSのリリース公表以後、堰を切ったようにブログやツイッターでこの件について警告を発信している。

業界関係者によると、JPRSは大手の事業者には水面下でこの問題を知らせ、対策を急がせているのではないかという。現に、JPRSとつながりの深いNTTグループのIIJの技術者が、なぜかこの問題について沈黙を守っている。IIJには優秀な「モノ言う技術者」が少なからずいて、この手の問題が勃発するとこれまでは積極的に議論する人が多かったのだが、今回はなぜか凪の海のように静かなのだ。

4月末にマイクロソフトのブラウザー「IE」（Internet Explorer）に脆弱性があることが発表されて大騒ぎとなった。マイクロソフト社はいち早く脆弱性を認め、米国土安全保障省を通じて世界に警告した。おかげで多くの人が5月2日に配布された修正ソフトを急いで適用した。これがグローバルスタンダードの対応策だろう。

「jp」ドメインには「co.jp」「ne.jp」といった事業系だけでなく「go.jp」という政府系ドメインも含まれる。それが無防備というのでは、「jp」ドメインを独占的に管理運用し利権を独り占めするJPRSは、国益に無自覚すぎないか。