NTTデータ 先端技術株式会社

Poison Ivy C&C サーバにおける、任意のコードが実行される脆弱性に関する検証レポート

2012/07/25
NTT データ先端技術株式会社
辻　伸弘
津田　尚彦

【概要】

Remote Administration Tool である Poison Ivy C&C サーバには、リモートから任意のコードが実行される脆弱性が存在します。
本脆弱性により、攻撃者が細工したパケットを攻撃対象ユーザに送信することで、Poison Ivy C&C サーバの実行ユーザ権限と同じ権限が奪取される危険性があります。
今回、この Poison Ivy C&C サーバの脆弱性の再現性について検証を行いました。

【影響を受けるとされているシステム】

影響を受ける可能性が報告されているのは次の通りです。
・Poison Ivy 2.3.2

【対策案】

本レポート作成現在(2012 年 7 月 25 日)、作者から脆弱性についてのアナウンス、及び修正プログラムのリリースはされておらず、ただいま対応策及び修正プログラムのリリース予定の有無を作者に問い合わせしております。返信がありましたら追って掲載する予定です。
また、現時点で公開されている情報によると、C&C サーバ/クライアント間の通信は、予め両者の間で設定されたパスワードによって暗号化されており、本脆弱性を利用するためには、そのパスワードを知っている必要があります。
そのため、対策として C&C サーバ/クライアント間で設定するパスワードを、デフォルト値である"admin"から、推測されにくい複雑なパスワードに変更することが挙げられますが、こちらの対策があまり意味をなさないものであるということが弊社の検証結果から判明いたしました。詳細は本レポートの最後の項目【付録】をご参照ください。

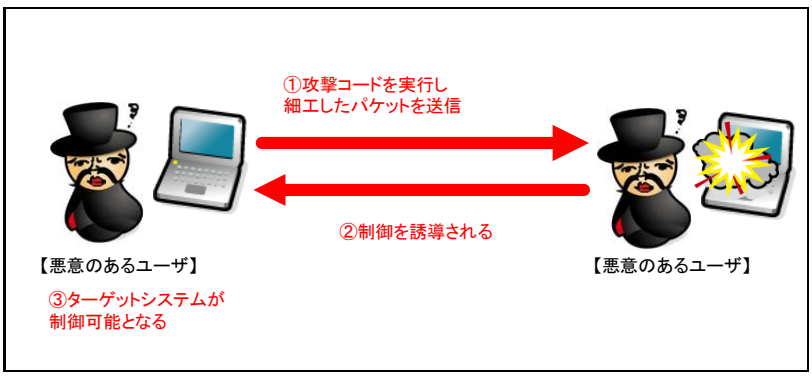
ここまで、Poison Ivy を使用するという前提で対策案をご提示いたしましたが最も確実である対策案は、そもそもこのようなプログラムは使用しないことです。

【参考サイト】

Own And You Shall Be Owned - Security Bits
http://badishi.com/own-and-you-shall-be-owned/

83774 Poison Ivy C&C Server Packet Header Handling Remote Overflow
http://www.osvdb.org/show/osvdb/83774

【検証イメージ】



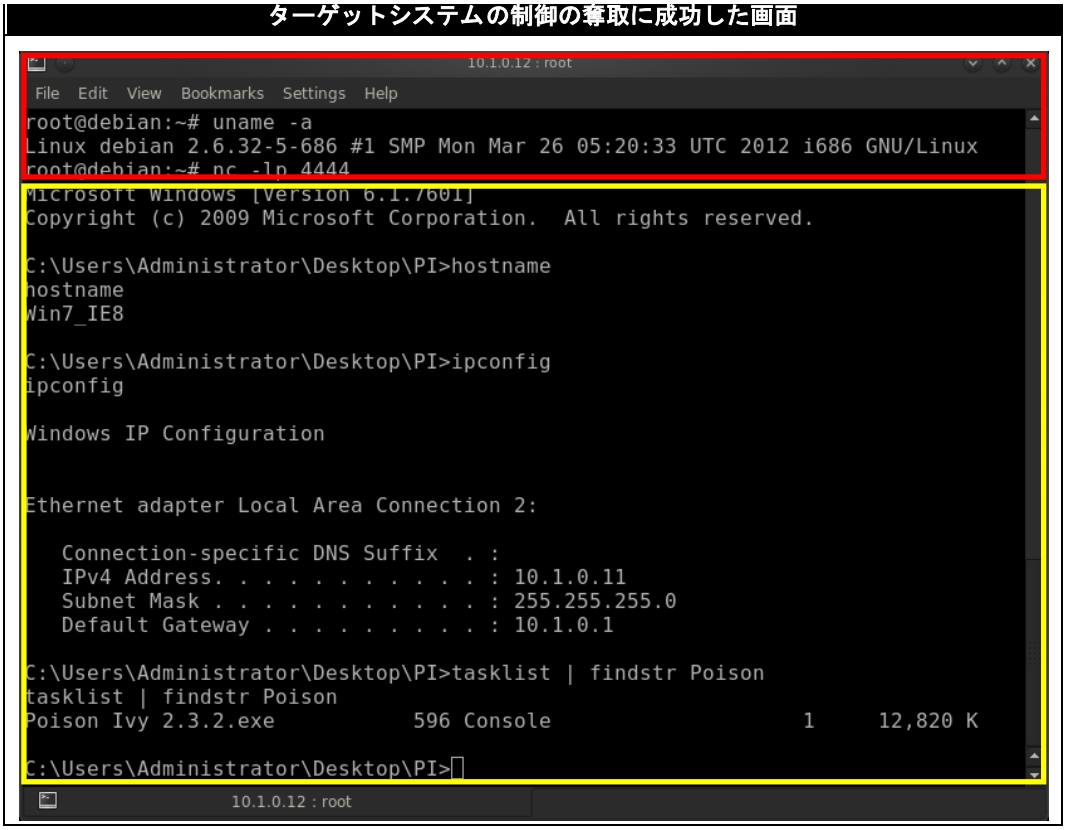
NTTデータ 先端技術株式会社

【検証ターゲットシステム】
・Windows 7 SP1
・Poison Ivy 2.3.2
＊C&C サーバ/クライアント間のパスワードは” admin”（デフォルト値）

【検証概要】
ターゲットシステムに、細工したパケットを送信することで任意のコードを実行させます。
今回の検証に用いたコードは、ターゲットシステム上から特定のサーバ、ポートへコネクションを確立させるよう誘導し、システムの制御を奪取するものです。
これにより、リモートからターゲットシステムを操作可能となります。
＊誘導先のシステムは Debian 6.0 です。

【検証結果】
下図の赤線で囲まれている部分の示すように、誘導先のコンピュータ（Debian）のコンソール上にターゲットシステム（Windows 7）のプロンプトが表示されています。
黄線で囲まれている部分の示すように、ターゲットシステムにおいて、コマンドを実行した結果が表示されています。
これにより、ターゲットシステムの制御の奪取に成功したと言えます。

ターゲットシステムの制御の奪取に成功した画面



【付録】

現在、公開されている攻撃コードには、C&C サーバ/クライアント間で予め設定されたパスワードが不明な場合にも総当たりによる攻撃を行う機能が実装されております。
本検証ターゲットシステムに対して、このオプションについての成功確率の検証も行いました。
下表がその結果になります。

総当たりの検証回数 / パスワード	1回目	2回目	3回目	4回目	5回目
a	Try1	Try4	Try4	失敗	Try5
z	Try1	Try1	Try1	Try1	Try1
aa	Try1	Try1	Try1	Try1	Try1
aaa	Try1	Try1	Try1	Try1	Try1
aaaa	Try2	失敗	Try3	Try3	失敗
intellilink.co.jp	Try1	Try1	Try1	Try1	Try1
nek0g@suk1	Try4	失敗	Try2	Try4	Try5
098f6bcd4621d373cade4e832627b4f6	失敗	Try3	Try5	Try2	失敗

縦軸は設定したパスワード、横軸は検証回数を表しております。また、検証1回毎に5回の攻撃試行を行っております。「Try」に続く数字は、攻撃に成功した際の攻撃試行回数を示しております。
例えば、縦軸「aaaa」、横軸「3回目」に当たるセルに「Try3」と表記されている場合は
「aaaa」という文字列が設定されている状態のPoison Ivy C&Cサーバに対して
「3回目」の検証の「3回」の攻撃試行の際に制御を奪取することに成功した。
ということを表します。また、「失敗」と表記されている場合は5回の攻撃試行では制御の奪取に至らなかったことを表しています。

上表のように非常に高い確率で成功してしまう結果となりました。
これにより C&C サーバ/クライアント間で設定するパスワードを複雑なパスワードに変更することは、対策と呼べるレベルではないと判断できます。

＊各規格名、会社名、団体名は、各社の商標または登録商標です。

【お問合せ先】

NTT データ先端技術株式会社
セキュリティ事業部　営業担当　サービス企画戦略グループ
TEL:03-5859-5422
http://security.intellilink.co.jp