攻撃グループLazarusが侵入したネットワーク内で使用するツール - JPCERT/CC Eyes | JPCERTコーディネーションセンター公式ブログ

blogs.jpcert.or.jp/ja/2021/01/Lazarus_tools.html

朝長 秀誠 (Shusei Tomonaga)

2021/01/19

攻撃グループLazarusが侵入したネットワーク内で使用するツール

Lazarus

-
- メール

攻撃者がネットワーク内に侵入した後、ネットワーク内の調査や感染拡大などにWindowsコマンドや正規のツールを使用することはよく知られています。攻撃グループLazarus（Hidden Cobraとも言われる）も同じく、ネットワークに侵入後、正規のツールを使用して、情報収集や感染拡大を試みます。
今回は、攻撃グループLazarusが使用するツールについて紹介します。

ネットワーク内部での横展開

まずは、ネットワーク内部での横展開（Lateral Movement）に使用されるツールです。AdFindはActive DirectoryからWindowsネットワーク内のクライアントやユーザーの情報を収集することが可能なツールで攻撃グループLazarusに限らず他の攻撃者でも使用されていることが確認されています[1]。SMBMapについては、以前のブログで紹介したとおり、マルウェアを別のホストに感染させるために使用しています。さらに、Responder-Windowsを使ってネットワーク内部の情報を収集していたことも確認されています。

ツール名	内容	参考
AdFind	Active Directoryから情報を収集するコマンドラインツール	http://www.joeware.net/freetools/tools/adfind/
SMBMap	ネットワーク内のアクセス可能なSMB共有を一覧したり、アクセスしたりするツール	https://github.com/ShawnDEvans/smbmap
Responder-Windows	LLMNR、NBT-NS、WPADになりすまして、クライアントを誘導するツール	https://github.com/lgandx/Responder-Windows

情報窃取

情報窃取に使用されるツールは以下の3つです。マルウェアに多くの情報窃取機能が搭載されているため、ツールが使用される場面は限られています。その中でもブラウザーやメーラーのアカウント情報を収集するためのツールが使用されています。また、情報を持ち出す際にファイルなどをRAR形式に圧縮するのが、よく見られる攻撃者のパターンですが、攻撃グループLazarusでも同じくWinRARを使用してファイルの圧縮を行っています。なお、以前のブログで記載したとおりマルウェア自体にzlib形式でファイル圧縮して送信する機能も持っているため、RAR形式以外で情報が送信されることもあります。

ツール名	内容	参考
XenArmor Email Password Recovery Pro	メールクライアントやサービスのパスワード情報を抽出するツール	https://xenarmor.com/email-password-recovery-pro-software/
XenArmor Browser Password Recovery Pro	ブラウザーに保存されたパスワード情報を抽出するツール	https://xenarmor.com/browser-password-recovery-pro-software/
WinRAR	RAR圧縮ツール	https://www.rarlab.com/

その他

最後にその他のツールです。攻撃者はRDPやTeamViewer、VNCなどを使用して感染したネットワーク内にバックドアを仕掛けることがよくあります。攻撃グループLazarusもVNCを使用する場合があることを確認しています。さらに、マイクロソフト純正ツールであるProcDumpを使用していたことも確認しています。ProcDump は、攻撃者がLSASSプロセスのダンプから、ユーザーの認証情報を抽出するために使用されることがあります。
その他に、tcpdumpやwgetなどLinuxではお馴染みのコマンドのWindows版ツールも使用されています。

ツール名	内容	参考
TightVNC Viewer	VNCクライアント	https://www.tightvnc.com/download.php
ProcDump	プロセスのメモリダンプを取得するマイクロソフト純正ツール	https://docs.microsoft.com/en-us/sysinternals/downloads/procdump
tcpdump	パケットキャプチャツール	https://www.tcpdump.org/
wget	ダウンロードツール	

おわりに

今回は、攻撃グループLazarusが使用するマルウェアではなくツールについて紹介しました。攻撃グループLazarusが使用するマルウェアは、これまで説明したとおり多機能ではありますが、足りないものは正規のツールを悪用していることが確認されています。このような正規のツールはウイルス対策ソフトで検知できないこともあるため、注意が必要です。
なお、今回解説したツールのハッシュ値に関しては、Appendix Aに記載していますので、ご覧ください。

インシデントレスポンスグループ 朝長 秀誠

参考情報

［1］Cybereason: Dropping Anchor: From a TrickBot Infection to the Discovery of the Anchor Malware
https://www.cybereason.com/blog/dropping-anchor-from-a-trickbot-infection-to-the-discovery-of-the-anchor-malware

Appendix A: ハッシュ値

注意: ここで記載するハッシュ値は正規のツールが多数含まれているため、インディケータとして使用する際は注意してください。

AdFind

- CFD201EDE3EBC0DEB0031983B2BDA9FC54E24D244063ED323B0E421A535CFF92
- B1102ED4BCA6DAE6F2F498ADE2F73F76AF527FA803F0E0B46E100D4CF5150682
- CFD201EDE3EBC0DEB0031983B2BDA9FC54E24D244063ED323B0E421A535CFF92

SMBMap

- 65DDF061178AD68E85A2426CAF9CB85DC9ACC2E00564B8BCB645C8B515200B67
- da4ad44e8185e561354d29c153c0804c11798f26915274f678db0a51c42fe656

Responder-Windows

- 7DCCC776C464A593036C597706016B2C8355D09F9539B28E13A3C4FFCDA13DE3
- 47D121087C05568FE90A25EF921F9E35D40BC6BEC969E33E75337FC9B580F0E8

XenArmor Email Password Recovery Pro

85703EFD4BA5B691D6B052402C2E5DEC95F4CEC5E8EA31351AF8523864FFC096

XenArmor Browser Password Recovery Pro

4B7DE800CCAEDEE8A0EDD63D4273A20844B20A35969C32AD1AC645E7B0398220

Winrar

- CF0121CD61990FD3F436BDA2B2AFF035A2621797D12FD02190EE0F9B2B52A75D
- EA139458B4E88736A3D48E81569178FD5C11156990B6A90E2D35F41B1AD9BAC1

TightVNC Viewer

- A7AD23EE318852F76884B1B1F332AD5A8B592D0F55310C8F2CE1A97AD7C9DB15
- 30B234E74F9ABE72EEFDE585C39300C3FC745B7E6D0410B0B068C270C16C5C39

Tcpdump

- 2CD844C7A4F3C51CB7216E9AD31D82569212F7EB3E077C9A448C1A0C28BE971B
- 1E0480E0E81D5AF360518DFF65923B31EA21621F5DA0ED82A7D80F50798B6059

Procdump

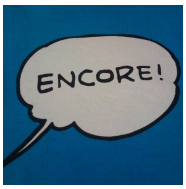
- 5D1660A53AAF824739D82F703ED580004980D377BDC2834F1041D512E4305D07
- F4C8369E4DE1F12CC5A71EB5586B38FC78A9D8DB2B189B8C25EF17A572D4D6B7

Wget

- C0E27B7F6698327FF63B03FCCC0E45EFF1DC69A571C1C3F6C934EF7273B1562F
- CF02B7614FEA863672CCBED7701E5B5A8FAD8ED1D0FAA2F9EA03B9CC9BA2A3BA

-
- メール

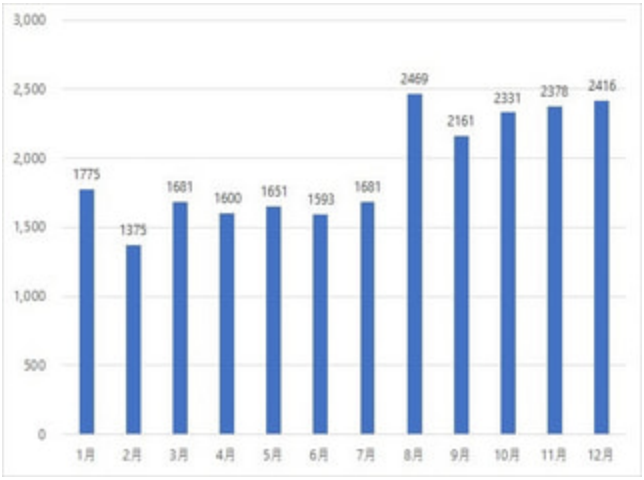
この記事の筆者



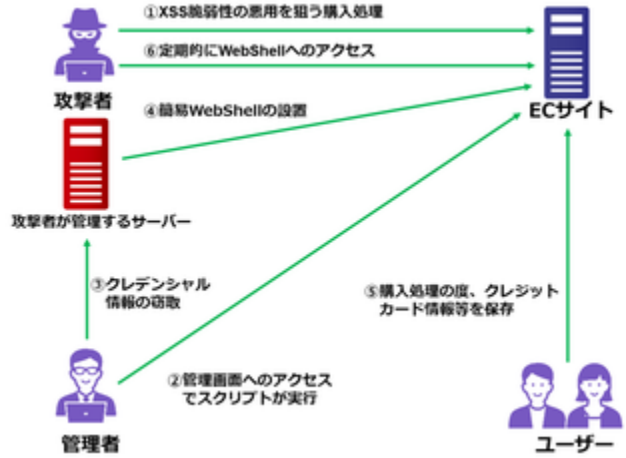
朝長 秀誠 (Shusei Tomonaga)

外資系ITベンダーでのセキュリティ監視・分析業務を経て、2012年12月から現職。現在は、マルウェア分析・フォレンジック調査に従事。主に、標的型攻撃に関するインシデント分析を行っている。CODE BLUE、BsidesLV、BlackHat USA Arsenal、Botconf、PacSec、FIRSTなどで講演。JSACオーガナイザー。

関連記事

- 

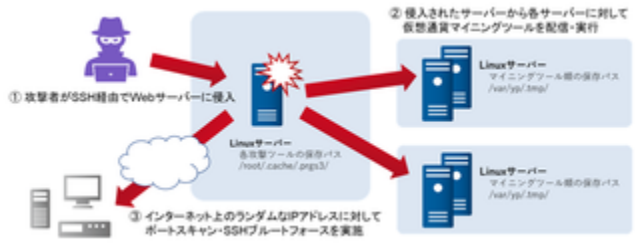
2021年に報告されたフィッシングサイトの傾向と利用されたドメインについて

- 

ECサイトのクロスサイトスクリプティング脆弱性を悪用した攻撃

- 

ラッキービジター詐欺で使用されるPHPマルウェア

- 

仮想通貨マイニングツールの設置を狙った攻撃

```
v7 = mal_check_count(http_strc->URL);
(*(void (__stdcall **)(int, int, int, int *))o_InternetCrackUrlA[0])(http_strc->URL, v7,
if ( v6 == 1 )
{
  wsprintfA(
    &v30,
    "Content-Type: multipart/form-data; boundary=%s\r\n",
    (const char *)http_strc->http_bonday_str);
  if ( !v20 || !v21 )
  {
    if ( v20 )
      wsprintfA(
        &v32,
        "--%s\r\nContent-Disposition: form-data; name=\"%s\"\r\n\r\n%s\r\n\r\n",
        (const char *)http_strc->http_bonday_str,
        (const char *)http_strc->http_name1,
        (const char *)http_strc->http_body_text);
    else
      wsprintfA(
        &v32,
        "--%s\r\n"
        "Content-Disposition: form-data; name=\"%s\"; filename=\"%s\"\r\n"
        "Content-Type: image/bmp\r\n"
        "\r\n",
        (const char *)http_strc->http_bonday_str,
        (const char *)http_strc->http_name,
        (const char *)http_strc->http_filename);
  }
  else
  {
    wsprintfA(
      &v32,
      "--%s\r\n"
      "Content-Disposition: form-data; name=\"%s\"\r\n"
      "\r\n"
      "%s\r\n"
      "--%s\r\n"
      "Content-Disposition: form-data; name=\"%s\"; filename=\"%s\"\r\n"
      "Content-Type: image/bmp\r\n"
      "\r\n",
      (const char *)http_strc->http_bonday_str,
      (const char *)http_strc->http_name1,
      (const char *)http_strc->http_body_text,
      (const char *)http_strc->http_bonday_str,
      (const char *)http_strc->http_name,
      (const char *)http_strc->http_filename);
  }
  wsprintfA(&v33, "\r\n--%s--\r\n", (const char *)http_strc->http_bonday_str);
  v27 = mal_check_count((int)&v32);
  v28 = mal_check_count((int)&v33);
```

- 日本の組織を狙った攻撃グループLazarusによる攻撃オペレーション

≪ 前へ
トップに戻る
次へ ≫