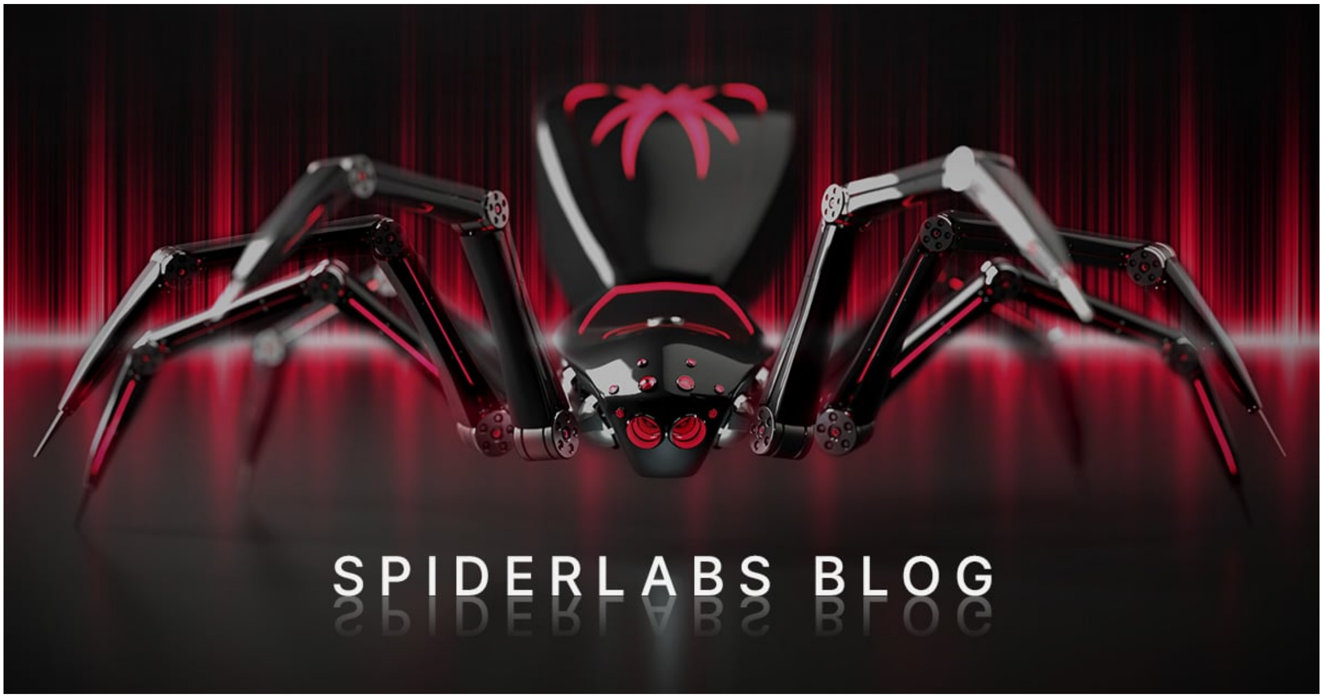
Proton66 Part 1: Mass Scanning and Exploit Campaigns



April 14, 2025 4 Minute Read by Pawel Knapczyk, Dawid Nesterowicz

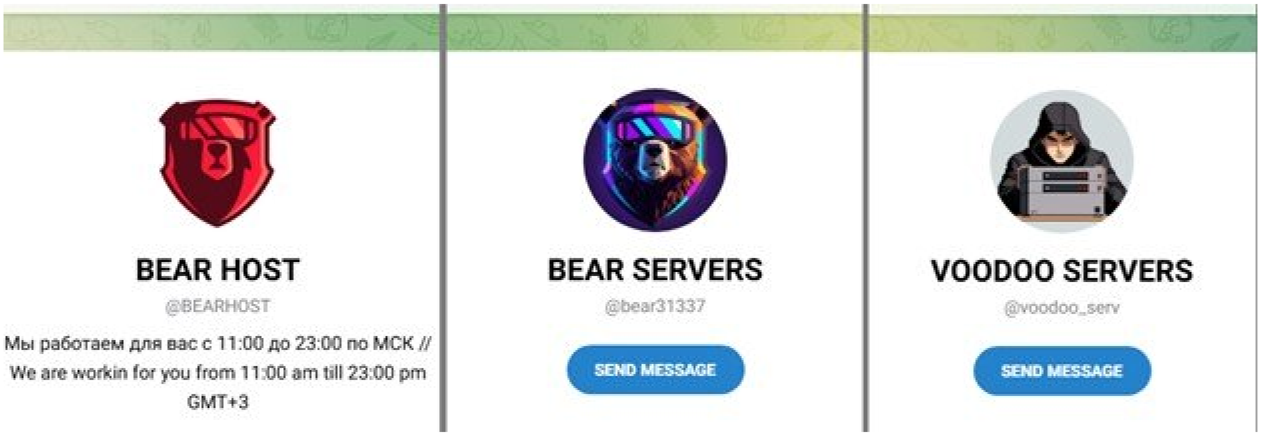
Trustwave SpiderLabs continuously tracks a range of malicious activities originating from Proton66 ASN, including vulnerability scanning, exploit attempts, and phishing campaigns leading to malware infections.

In this two-part series, SpiderLabs explores the malicious traffic associated with Proton66, revealing the extent and nature of these attacks. The first part of the series focuses on mass scanning and exploit activities, highlighting a specific IP address connected to SuperBlack ransomware operators, found to distribute some of the latest critical priority exploits.

The second part delves into a range of malware campaigns linked to Proton66, including compromised WordPress websites redirecting Android devices to fake Google Play stores, an XWorm campaign targeting Korean-speaking chat room users, and the WeaXor Ransomware.

Underground Hosting Services

In November 2024, the security firm Intrinsec detailed how PROSPERO (AS200593) and Proton66 (AS198953) are connected to bulletproof services advertised on underground forums under the names UNDERGROUND and BEARHOST. Multiple malware campaigns were mentioned, with some of the IP addresses changing between networks. Interested customers could reach out via dedicated Telegram or Jabber accounts offering both Russian and English.

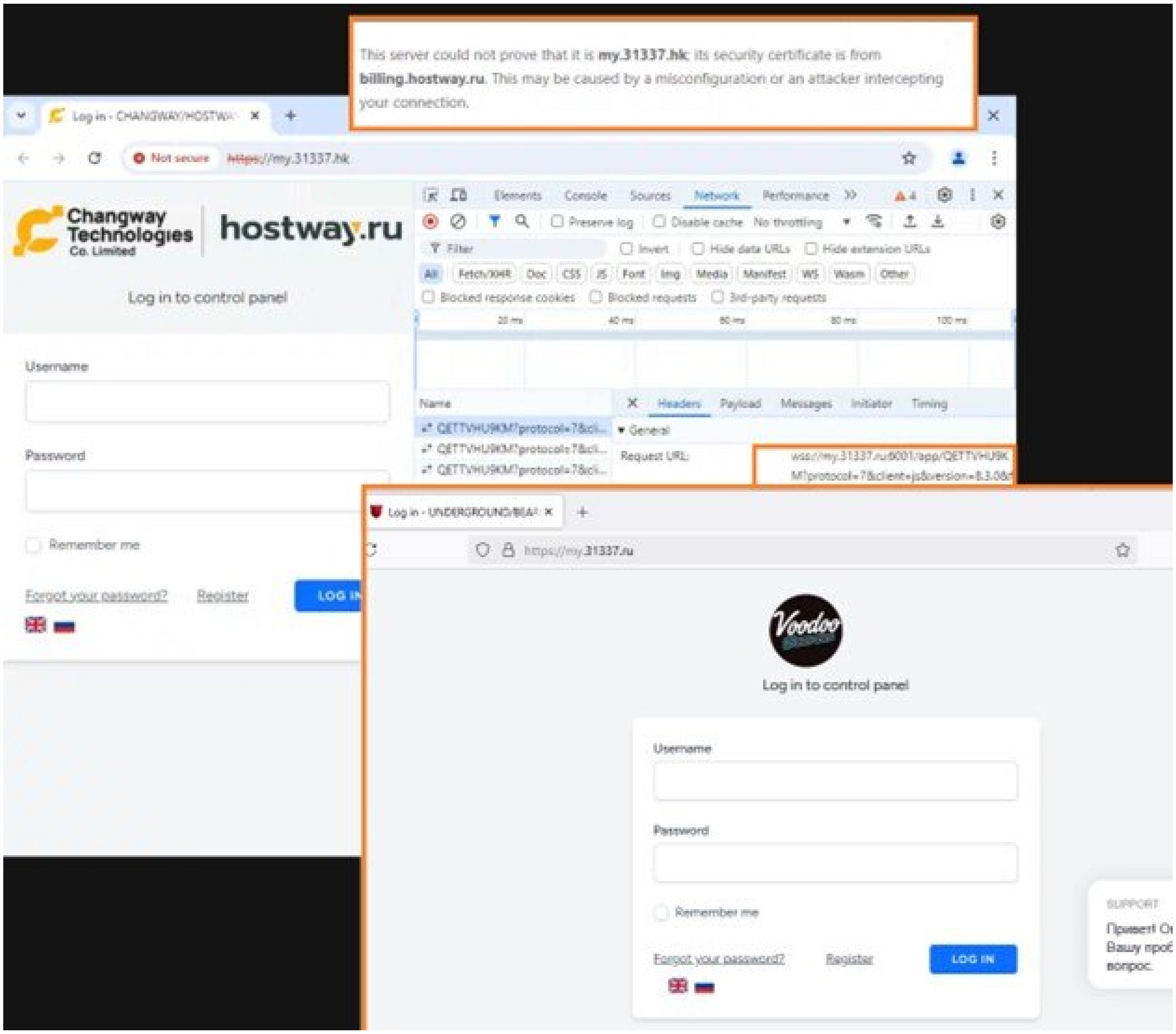


Мы работаем для вас с 11:00 до 23:00 по МСК // We are workin for you from 11:00 am till 23:00 pm GMT+3

Figure 1. Telegram accounts operating bulletproof services as BEARHOST/UNDERGROUND. Source: SpiderLabs.

In December 2024, a thread offering hosting services from UNDERGROUND/BEARHOST disappeared from one of the major underground forums. This, of course, confused some users, and they started to ask questions. A user named “Voodo_servers” responded to one of those inquiries, stating that the services are now offered through a private company, and customers are no longer being recruited through the forums. Intrinsec’s research had already drawn indirect connections between BEARHOST/UNDERGROUND and Hong Kong-based Chang Way Technologies Co. Limited, however, SpiderLabs’ investigation revealed another interesting piece of evidence suggesting a rebranding.

While the Russian hosting control panel used by UNDERGROUND BEARHOST customers, my.31337.ru, remained unchanged, my.31337.hk page was updated to a new CHANGWAY / HOSTWAY theme. However, a websocket connection to my.31337.ru:6001 opened by the panel application script was visible in the background, indicating that the underlying infrastructure is interlaced. Interestingly, likely due to misconfiguration, a certificate from billing.hostway.ru was served by my.31337.hk at the time of research.


This server could not prove that it is **my.31337.hk**; its security certificate is from **billing.hostway.ru**. This may be caused by a misconfiguration or an attacker intercepting your connection.

Request URL: wss://my.31337.ru:6001/app/QETTVHU9KM?protocol=7&client=js&version=8.3.0&

Figure 2. Bearhost/Underground rebranding to Changway/Hostway. Source: SpiderLabs.

SpiderLabs also observed an IP address shift from Proton66 ASN to Chang Way Technologies ASN in campaigns leveraging compromised WordPress pages discussed in Part 2, suggesting a relation between both providers.

Mass scanning and exploit campaigns targeting multiple sectors

Starting from January 8, 2025, SpiderLabs observed an increase in mass scanning, credential brute forcing, and exploitation attempts originating from Proton66 ASN targeting organizations worldwide. Although malicious activity was seen in the past, the spike and sudden decline observed later in February 2025 were notable, and offending IP addresses were investigated.

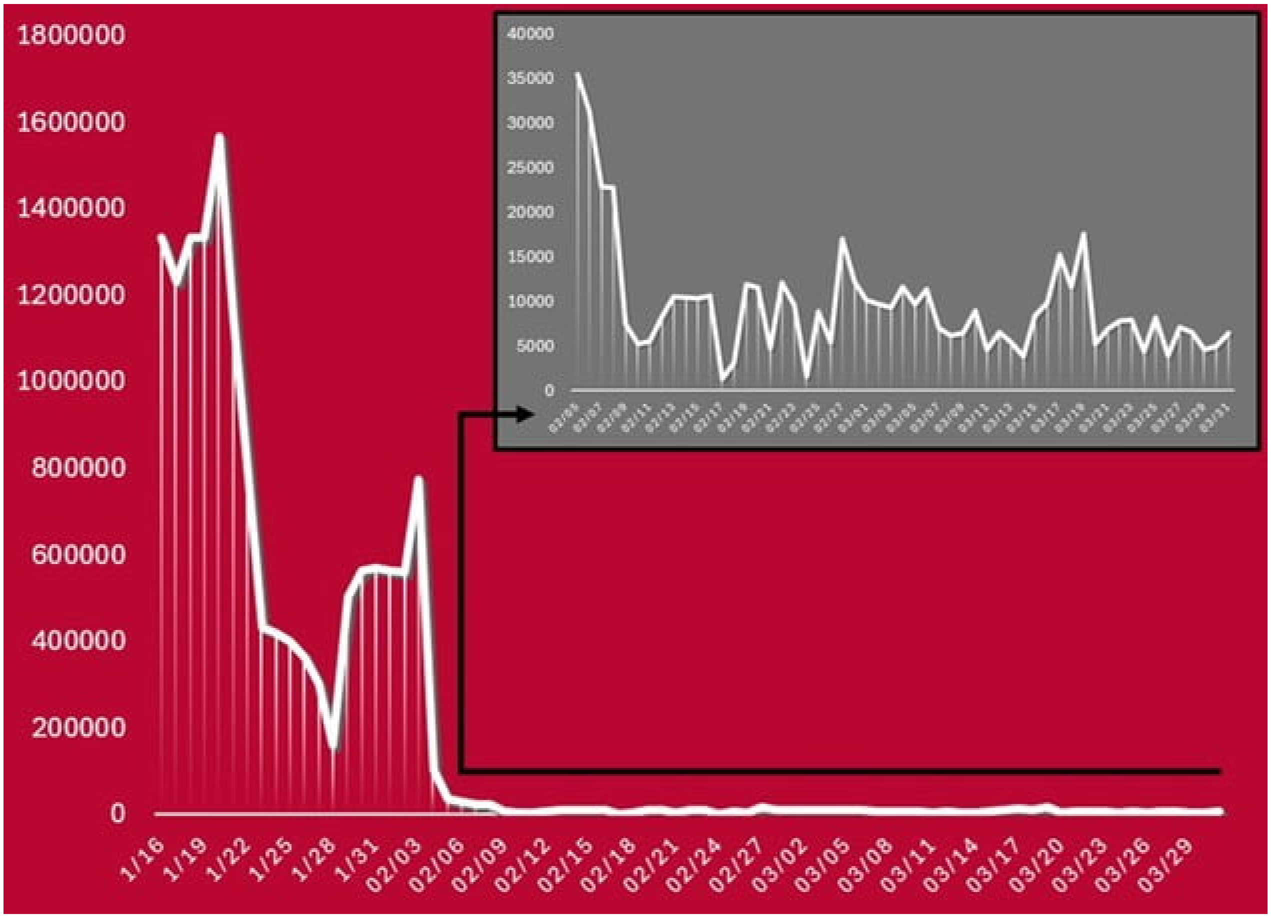


Figure 3. Volume of the scanning and exploit traffic originating from Proton66 ASN. Source: SpiderLabs.

AS198953, belonging to Proton66 OOO, consists of five net blocks, which are currently listed on blocklists such as Spamhaus due to malicious activity. Net blocks 45.135.232.0/24 and 45.140.17.0/24 were particularly active in terms of mass scanning and brute force attempts. Several of the offending IP addresses were not previously seen to be involved in malicious activity or were inactive for over two years. For instance, the last activities reported in AbuseIPDB for the IP addresses 45.134.26.8 and 45.135.232.24 were noted in November and July 2021, respectively.

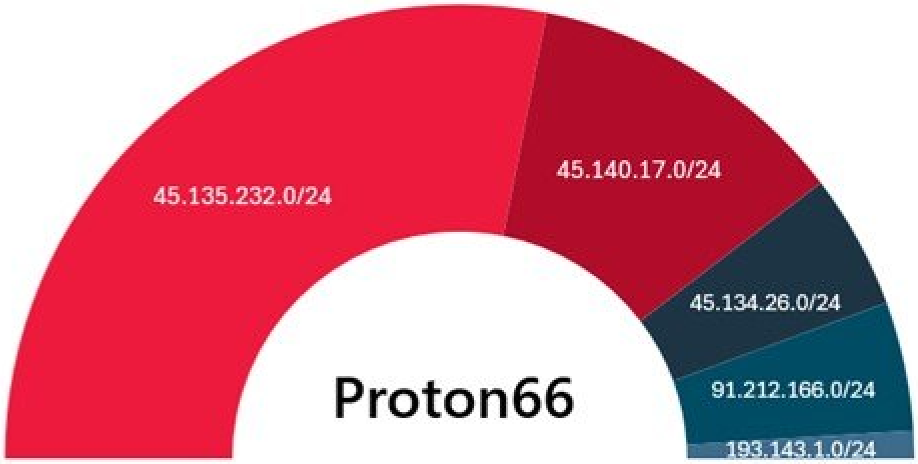


Figure 4. Scanning and exploit traffic volume originating from Proton66 net blocks (Jan. to Mar. 2025). Source: SpiderLabs.

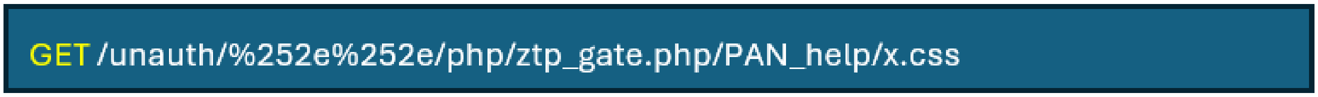
Statistics collected between January and March indicated that technology and financial organizations were, in general, the most common target for these activities. The majority of these scanning and exploit attempts have already been blocked at the time of research, mitigating the exploitation risk for our customers.

SuperBlack Ransomware Operator Takes Advantage of Newest Vulnerabilities

Malicious requests originating from 193.143.1.65. observed by SpiderLabs in February 2025 were particularly interesting, aiming to exploit some of the most recent critical vulnerabilities:

CVE-2025-0108: An authentication bypass in the management web interface of Palo Alto Networks’ PAN-OS software, enabling an unauthenticated attacker with network access to the management web interface to bypass the authentication otherwise required by the PAN-OS management web interface and invoke certain PHP scripts.

URL request observed in exploit attempts:

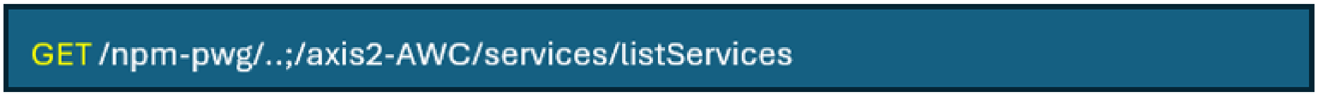


```
GET /unauth/%252e%252e/php/ztp_gate.php/PAN_help/x.css
```

Figure 5. URL request observed in exploit attempts.

CVE-2024-41713: A vulnerability in Mitel MiCollab 9.8 SP1 FP2 (9.8.1.201) allowing an unauthenticated attacker to conduct a path traversal attack due to insufficient input validation. A successful exploit could allow unauthorized access, enabling the attacker to view, corrupt, or delete users' data and system configurations.

URL request observed in exploit attempts:

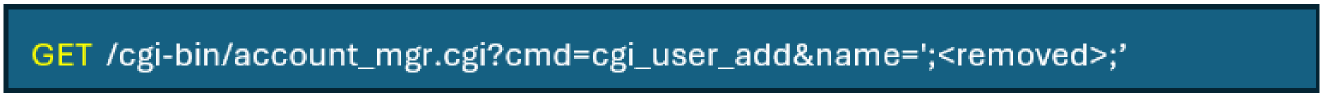


```
GET /npm-pwg/..;/axis2-AWC/services/listServices
```

Figure 6. URL request observed in exploit attempts.

[CVE-2024-10914](https://www.cve.org/CVERecord?id=CVE-2024-10914): A command injection vulnerability D-Link NAS that allows unauthenticated attackers to inject arbitrary commands by exploiting the name parameter in the *cgi_user_add* command. This issue affects the following D-Link NAS models: D-Link DNS-320, DNS-320LW, DNS-325, and DNS-340L. Since these devices have reached their end of life (EOL), D-Link has not provided any updates, as all development and customer support have been discontinued.

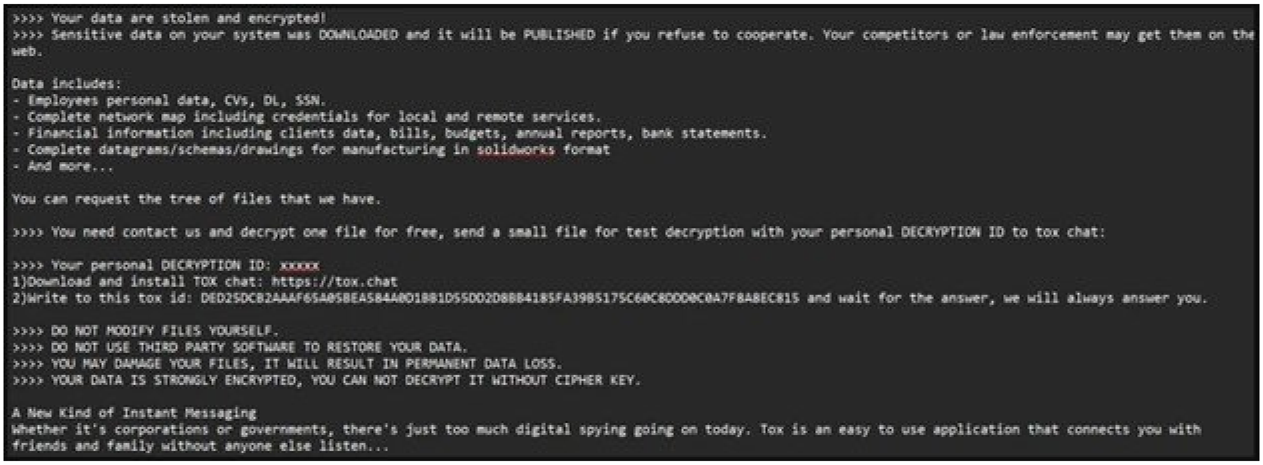
- https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10413
- URL request observed in exploit attempts:



```
GET /cgi-bin/account_mgr.cgi?cmd=cgi_user_add&name=';<removed>;'
```

Figure 7. URL request observed in exploit attempts.

A research document published by Forescout in March, links 193.143.1.65 with activities performed by a new ransomware operator and likely an initial access broker, dubbed “Mora_001”, seen exploiting critical authentication bypass vulnerabilities affecting Fortinet FortiOS-based devices (CVE-2024-55591 and CVE-2025-24472). The intrusion following FortiOS exploitation led to the deployment of a new ransomware strain dubbed “SuperBlack”, which closely resembles LockBit 3.0. The main differences lie in the ransom note left after encryption and the custom data exfiltration executable.



```
>>>> Your data are stolen and encrypted!
>>>> Sensitive data on your system was DOWNLOADED and it will be PUBLISHED if you refuse to cooperate. Your competitors or law enforcement may get them on the
web.

Data includes:
- Employees personal data, CVs, DL, SSN.
- Complete network map including credentials for local and remote services.
- Financial information including clients data, bills, budgets, annual reports, bank statements.
- Complete datagrams/schemas/drawings for manufacturing in solidworks format
- And more...

You can request the tree of files that we have.

>>>> You need contact us and decrypt one file for free, send a small file for test decryption with your personal DECRYPTION ID to tox chat:

>>>> Your personal DECRYPTION ID: xxxxx
1)Download and install TOX chat: https://tox.chat
2)Write to this tox id: DED25DCB2AAAF65A05BEA584A0D1BB1D55DD2D8BB4185FA39B5175C60C8DDD0C0A7F8A8EC815 and wait for the answer, we will always answer you.

>>>> DO NOT MODIFY FILES YOURSELF.
>>>> DO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.
>>>> YOU MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.
>>>> YOUR DATA IS STRONGLY ENCRYPTED, YOU CAN NOT DECRYPT IT WITHOUT CIPHER KEY.

A New Kind of Instant Messaging
Whether it's corporations or governments, there's just too much digital spying going on today. Tox is an easy to use application that connects you with
friends and family without anyone else listen...
```

Figure 8. SuperBlack ransomware note. Source: Forescout Research.

SpiderLabs analyzed the sectors targeted by malicious traffic originating from the IP address 193.143.1.65, which is linked to “Mora_001”, between January and March and found that non-profit, engineering, and financial sectors were the attacker’s most preferred picks.

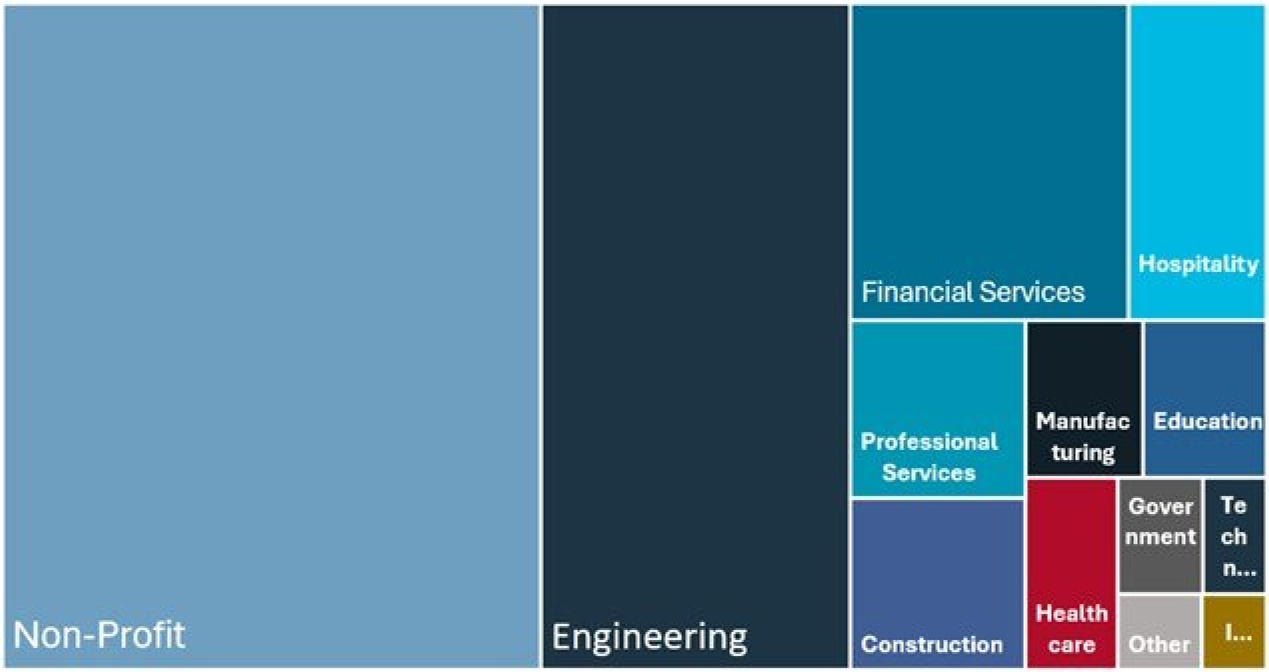


Figure 9. Sectors targeted by scans, brute force, and exploit attempts from 193.143.1.65. Source: SpiderLabs

All of our customers were protected as the scanning and exploit attempts were blocked.

In the second part, we will discuss malware campaigns linked to Proton66, including compromised WordPress websites redirecting Android devices to fake Google Play stores, an XWorm campaign targeting Korean chat room users, and the WeaXor ransomware.

Selected IOCs Observed (Scanning, Brute Force, and Exploitation):

Type	Value	Description
IP	45.134.26.38	Proton66
IP	45.140.17.21	Proton66
IP	45.140.17.98	Proton66
IP	45.135.232.108	Proton66
IP	45.135.232.171	Proton66
IP	45.135.232.174	Proton66

IP	45.135.232.103	Proton66
IP	45.135.232.24	Proton66
IP	45.134.26.80	Proton66
IP	45.134.26.81	Proton66
IP	45.134.26.104	Proton66
IP	45.134.26.124	Proton66
IP	45.134.26.199	Proton66
IP	45.134.26.8	Proton66
IP	91.212.166.65	Proton66
IP	91.212.166.62	Proton66
IP	91.212.166.60	Proton66
IP	91.212.166.27	Proton66
IP	193.143.1.78	Proton66
IP	193.143.1.33	Proton66
IP	193.143.1.64	Proton66

Selected IOCs Observed (Scanning, Brute Force, and Exploitation):

Type	Value	Decription	Actor
IP	193.143.1.65	Proton66	Mora_001