Elephant Hunting | Inside an Indian Hack-For-Hire Group

Tom Hegel ⁝

Executive Summary

- SentinelLabs has garnered new intelligence pertaining to the activities of the Appin Security Group, a renowned entity in the realm of hack-for-hire services.
- Our comprehensive analysis has unearthed information on numerous global cyber intrusions, encompassing instances of espionage, surveillance, and disruptive actions. Furthermore, our findings establish a high level of confidence in attributing intrusions in various countries, including Norway, Pakistan, China, and India, among others.
- The landscape of hack-for-hire enterprises has undergone a transformation, diversifying the array of services available to both private enterprises and government entities. Notwithstanding previous public disclosures, the internal methodologies governing the creation of malware, exploits, and network infrastructure have persisted in obscurity. Our investigative efforts contribute crucial insights, shedding light on the intricate processes underlying these operations.

Overview

Hack-for-Hire threat actors go by many names, such as surveillance-for-hire, mercenaries, private-sector-offensive-actors (PSOAs), and nonstate offensive threat actors. Such groups represent an interesting challenge for security researchers and network defenders, and should be considered a serious threat to all organizations, worthy of both proactive tracking in ongoing intrusions and analysis of historical cases to understand their significant impacts. Attempts to track and disrupt mercenary threat actors have been highlighted in many public industry reports, including our past work on Void Balaur and Meta's Surveillance-for-Hire report.

In this report, we share our findings from a review of highly unique, non-public, and technically-verified data into the hack-for-hire efforts of the Appin business. After an extensive review of this data, brought to our attention by Reuters investigative journalists, we assess with high confidence that it correlates with previously known Appin intrusions, accurately depicts internal communications, and originated from inside the security arm of the Appin organization– formally known as Appin Software Security and informally as Appin Security Group (ASG).

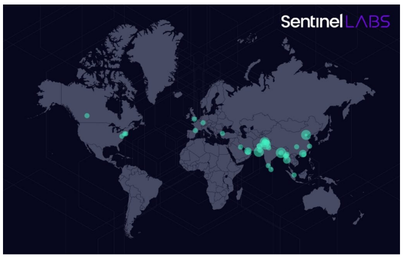
Introduction to Appin

Appin is considered the original hack-for-hire company in India, offering an offensive security training program alongside covert hacking operations since at least 2009. Their past employees have since spread to form newer competitors and partners, evolving the Appin brand to include new names, while some have spread into cybersecurity defense industry vendors. Appin was so prolific that a surprising amount of current Indian APT activity still links back to the original Appin group of companies in one form or another. Campaigns conducted by Appin have revealed a noteworthy customer base of government organizations, and private businesses spread globally.

Our analysis and observations corroborate the June 2022 reporting from Reuters noting some of Appin's customers tied to major litigation battles. The group has conducted hacking operations against high value individuals, governmental organizations, and other businesses involved in specific legal disputes. Appin's hacking operations and overall organization appear at many times informal, clumsy, and technically crude; however, their operations proved highly successful for their customers, impacting world affairs with significant success.

Victims, and Links to Previous Reporting

The extensive scope of unique targets and confirmed victims extends globally. The data reveals victims across the United States, Canada, China, India, Myanmar, Kuwait, Bangladesh, the United Arab Emirates, Pakistan, and other locations. The affected devices encompass those affiliated with both governmental entities and businesses across various industries. It is important to note that the aforementioned list is not exhaustive, serving as a snapshot at a particular moment rather than a comprehensive compilation of all targets and victims.



Victim Beacon Source IPs Visualized

From a threat intelligence perspective, the data includes details that identify specific victims of notable public interest. Attacks on China and Pakistan from India-linked threat actors are not new; however, the confirmation that a local Indian hack-for-hire group was enlisted to conduct these campaigns is insightful on the attribution of presumably state-sponsored attacks coming out of India. We can confirm some known victimology as well as observe additional previously undiscovered victims:

Pakistani Government Officials

These victims were successfully compromised and sent keylogger data from their machines to the Appin owned and controlled server. The keylogger data contained personal social media and email account logins, government website logins, and more mundane web browsing like travel, games, and pornography sites. Pakistani targeting continued in the years following, as reported by ESET in 2013 and noted in the below Operation Hangover report.

Chinese Government Officials

Multiple cases starting in 2009 involved data theft operations against Chinese government officials. These include the successful compromise of multiple PLA officers. Around the same time operators successfully compromised Military Liaison Officers with the same objective. Notably, these attacks were carried out shortly after Indian government officials made public statements they had observed cyber attacks on Indian government networks and attributed the activity to China.

Domestic Targeting

There are also many cases of domestic targeting. For example, in one case the Intelligence organization within a local police force enlisted Appin to conduct defacement attacks on specific Sikh websites and to steal login credentials of email accounts belonging to Sikhs in India and the U.S. One such inbound request reviewed contained a formal request document for Appin to break into the personal Gmail account of a specific individual, labeled as a domestic terrorist target. In an unrelated campaign, the group also used the domain `speedaccelator[.]com` for an FTP server, hosting malware used in their malicious phishing emails, one of which was used on an Indian individual later targeted by the ModifiedElephant APT.

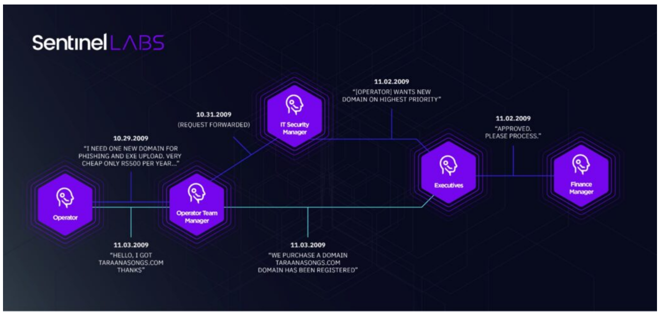
KitM Mac Spyware

In 2013, F-Secure analyzed and reported (1,2,3) on the technical details of Mac spyware originally discovered on the machine of an Angolan activist while visiting the Oslo Freedom Forum ("a global gathering of activists united in standing up to tyranny."). This Mac spyware was quite unique at the time, and ultimately dubbed KitM ('Kumar in the Mac', referring to the certificate issued under the name 'Rajinder Kumar', used to sign all of the samples), and made use of Appin owned and operated infrastructure. The newly reviewed data provided some of the context behind this campaign and the confirmation of actor attribution to Appin.

Operation Hangover

One of the more interesting links to previous reporting is the overlap with Operation Hangover. This 2013 report was a unique deepdive into threat activity around an industrial espionage campaign against the Norwegian telecommunications corporation, Telenor, along with other private companies. The authors note multiple strong links between the Appin organization and the attacks observed in-the-wild. Our new findings confirm that the malware and attack infrastructure noted in the Operation Hangover report were indeed owned and controlled by Appin, such as `taraanasongs[.]com` and others highlighted in here.

Below is a graphic depicting the process of acquiring Operation Hangover-related domains. In late October 2009, an operator requested a "new domain for phishing and exe upload" from their manager. The manager then forwarded the request, which made its way to executive staff and finance manager after approval. A day later the operator acknowledged the new domain (`taraanasongs[.]com`), and the manager informed the executive staff of its acquisition.


SentinelLABS
10.29.2009
"I NEED ONE NEW DOMAIN FOR PHISHING AND EXE UPLOAD. VERY CHEAP ONLY RS500 PER YEAR..."
10.31.2009
(REQUEST FORWARDED)
IT Security Manager
11.02.2009
"[OPERATOR] WANTS NEW DOMAIN ON HIGHEST PRIORITY"
11.02.2009
"APPROVED. PLEASE PROCESS."
Operator
Operator Team Manager
Executives
Finance Manager
11.03.2009
"HELLO, I GOT TARAANASONGS.COM THANKS"
11.03.2009
"WE PURCHASE A DOMAIN TARAANASONGS.COM DOMAIN HAS BEEN REGISTERED"

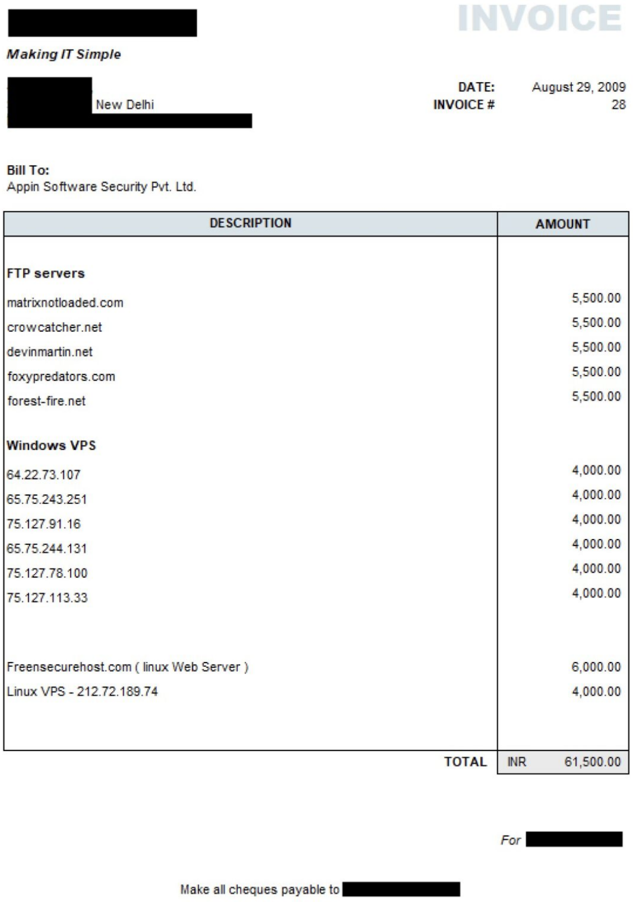
Appin Operator Requesting Purchase of *taraanasongs[.]com*

Infrastructure Acquisition and Use

Leading hack-for-hire organizations are faced with important segmentation requirements in order to limit the discovery of their infrastructure. If a researcher were to discover what connects all points of their infrastructure together, it would risk the entire set of customer operations.

Appin's method of acquiring and managing infrastructure for years was handled through a particular outside contractor. At the time, this individual would register the domains and set up hosting solutions as needed for a project. Appin operators would request a type of server, including some technical requirements, and which operator is assigned for its use.

The consultant would then purchase the server, set it up as instructed, provide credentials for remote access to the operator and Appin leadership, and conclude the interaction with an invoice detailing payment. Based on the data reviewed, the consultant made the purchases through a collection of repeated personal and business branded email accounts, in addition to overlapping registration and hosting details.



[redacted]
Making IT Simple

INVOICE

[redacted] New Delhi [redacted]

DATE: August 29, 2009
INVOICE # 28

Bill To:
Appin Software Security Pvt. Ltd.

DESCRIPTION	AMOUNT
FTP servers	
matrixnotloaded.com	5,500.00
crowcatcher.net	5,500.00
devinmartin.net	5,500.00
foxypredators.com	5,500.00
forest-fire.net	5,500.00
Windows VPS	
64.22.73.107	4,000.00
65.75.243.251	4,000.00
75.127.91.16	4,000.00
65.75.244.131	4,000.00
75.127.78.100	4,000.00
75.127.113.33	4,000.00
Freensecurehost.com (linux Web Server)	6,000.00
Linux VPS - 212.72.189.74	4,000.00
TOTAL	INR 61,500.00

For [redacted]

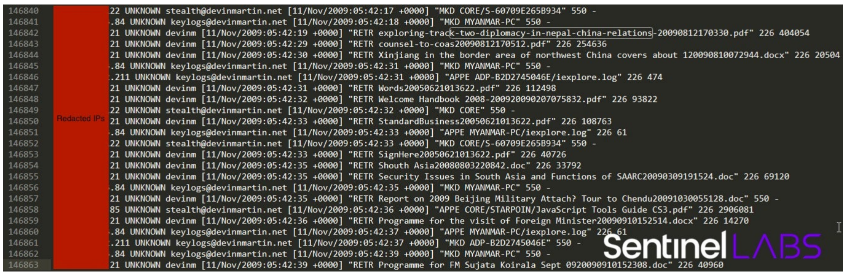
Make all cheques payable to [redacted]

Invoice to Appin for Malicious FTP Domains and VPS Servers

The types of servers requested generally centered around a handful of main purposes.

- **Exfiltration** – Often referred to as FTP servers or Data Transfer servers in the early years, malware would use these as the destination for exfiltrating stolen data. One may also find the logs of an Appin owned and operated exfiltration server useful for victim identification. For example, those originating from devinmartin[.]net highlight a global victim spread as previously noted. Data was uploaded to this specific FTP server with accounts:

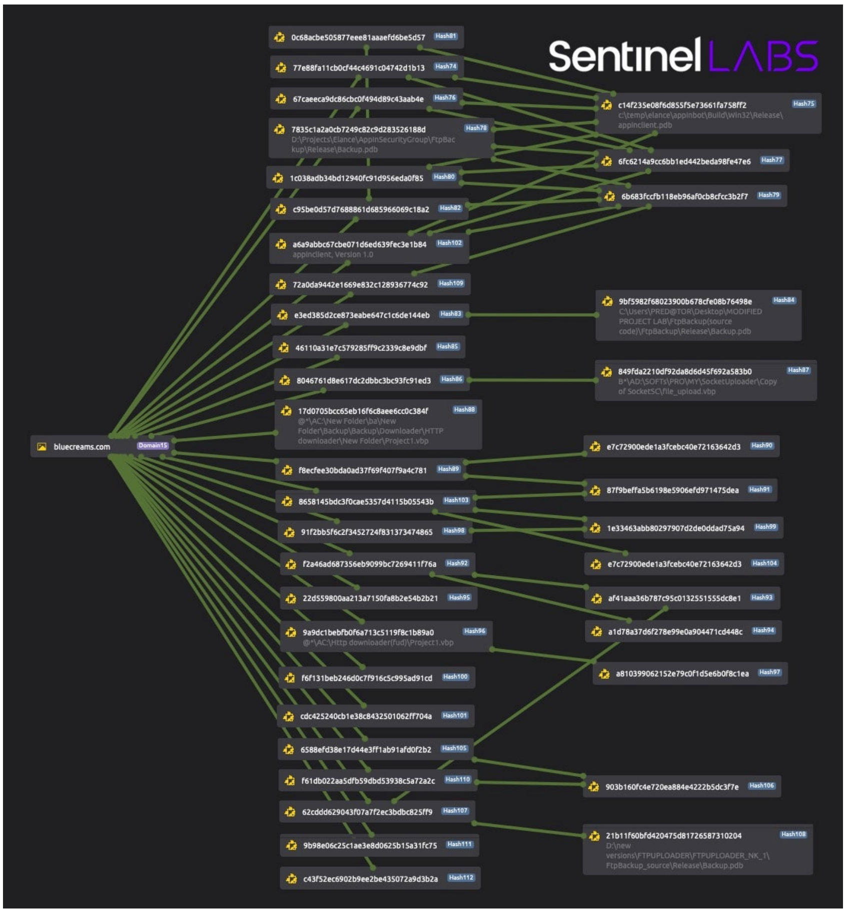
```
stealth@devinmartin[.]net
keylogs@devinmartin[.]net
radar@devinmartin[.]net
123456@devinmartin[.]net
devinmartin@devinmartin[.]net
revolution@devinmartin[.]net
devinmart@devinmartin[.]net
reloaded@devinmartin[.]net
cinema@devinmartin[.]net
lux@devinmartin[.]net
```



```
.22 UNKNOWN stealth@devinmartin.net [11/Nov/2009:05:42:17 +0000] "MKD CORE/S-60709E265B934" 550 -
.84 UNKNOWN keylogs@devinmartin.net [11/Nov/2009:05:42:18 +0000] "MKD MYANMAR-PC" 550 -
21 UNKNOWN devinm [11/Nov/2009:05:42:19 +0000] "RETR exploring-track-two-diplomacy-in-nepal-china-relations-20090812170330.pdf" 226 404054
21 UNKNOWN devinm [11/Nov/2009:05:42:29 +0000] "RETR counsel-to-coas20090812170512.pdf" 226 254636
21 UNKNOWN devinm [11/Nov/2009:05:42:30 +0000] "RETR Xinjiang in the border area of northwest China covers about 120090810072944.docx" 226 20504
.84 UNKNOWN keylogs@devinmartin.net [11/Nov/2009:05:42:31 +0000] "MKD MYANMAR-PC" 550 -
.211 UNKNOWN keylogs@devinmartin.net [11/Nov/2009:05:42:31 +0000] "APPE ADP-B2D2745046E/iexplore.log" 226 474
21 UNKNOWN devinm [11/Nov/2009:05:42:31 +0000] "RETR Words20050621013622.pdf" 226 112498
21 UNKNOWN devinm [11/Nov/2009:05:42:32 +0000] "RETR Welcome Handbook 2008-200920090207075832.pdf" 226 93822
.22 UNKNOWN stealth@devinmartin.net [11/Nov/2009:05:42:32 +0000] "MKD CORE" 550 -
21 UNKNOWN devinm [11/Nov/2009:05:42:33 +0000] "RETR StandardBusiness20050621013622.pdf" 226 108763
.84 UNKNOWN keylogs@devinmartin.net [11/Nov/2009:05:42:33 +0000] "APPE MYANMAR-PC/iexplore.log" 226 61
.22 UNKNOWN stealth@devinmartin.net [11/Nov/2009:05:42:33 +0000] "MKD CORE/S-60709E265B934" 550 -
21 UNKNOWN devinm [11/Nov/2009:05:42:33 +0000] "RETR SignHere20050621013622.pdf" 226 40726
21 UNKNOWN devinm [11/Nov/2009:05:42:35 +0000] "RETR Shouth Asia20080803220842.doc" 226 33792
21 UNKNOWN devinm [11/Nov/2009:05:42:35 +0000] "RETR Security Issues in South Asia and Functions of SAARC20090309191524.doc" 226 69120
.84 UNKNOWN keylogs@devinmartin.net [11/Nov/2009:05:42:35 +0000] "MKD MYANMAR-PC" 550 -
21 UNKNOWN devinm [11/Nov/2009:05:42:35 +0000] "RETR Report on 2009 Beijing Military Attach? Tour to Chendu20091030055128.doc" 550 -
85 UNKNOWN stealth@devinmartin.net [11/Nov/2009:05:42:36 +0000] "APPE CORE/STARPOIN/JavaScript Tools Guide CS3.pdf" 226 2906081
21 UNKNOWN devinm [11/Nov/2009:05:42:36 +0000] "RETR Programme for the visit of Foreign Minister20090910152514.docx" 226 14270
.84 UNKNOWN keylogs@devinmartin.net [11/Nov/2009:05:42:37 +0000] "APPE MYANMAR-PC/iexplore.log" 226 61
.211 UNKNOWN keylogs@devinmartin.net [11/Nov/2009:05:42:37 +0000] "MKD ADP-B2D2745046E" 550 -
.84 UNKNOWN keylogs@devinmartin.net [11/Nov/2009:05:42:39 +0000] "MKD MYANMAR-PC" 550 -
21 UNKNOWN devinm [11/Nov/2009:05:42:39 +0000] "RETR Programme for FM Sujata Koirala Sept 0920090910152308.doc" 226 40960
```

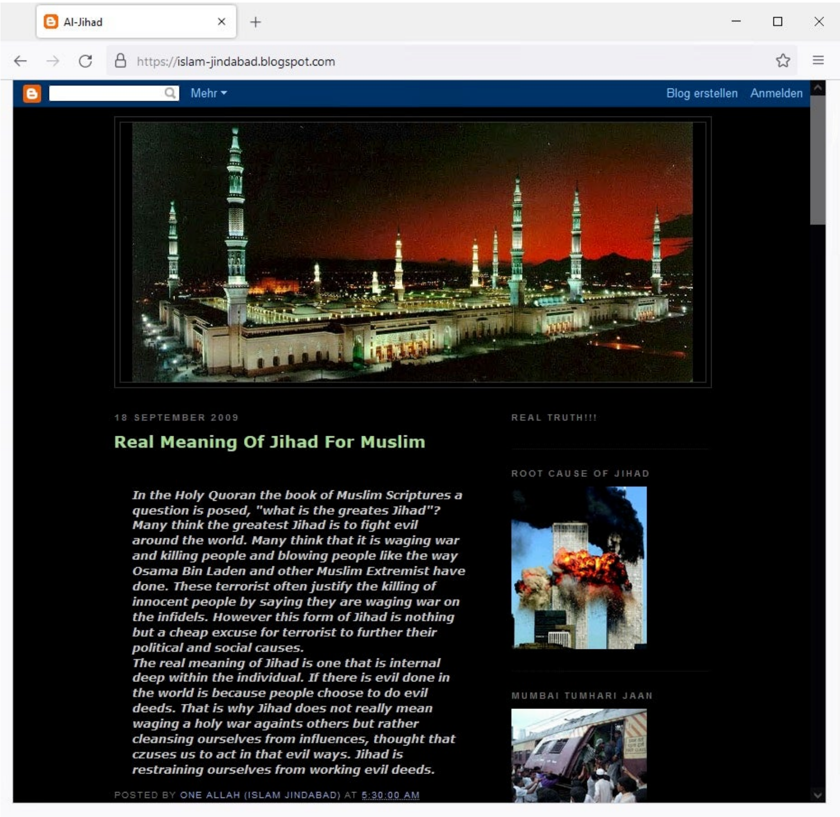
Data Exfiltration Logs from C2 server, with Victim IPs Redacted

- **C2 and Delivery Servers** – Malware command and control, or hosting malware for download.


bluecreams.com Domain15
0c68acbe505877eee81aaaefd6be5d57 Hash81
77e88fa11cb0cf44c4691c04742d1b13 Hash74
67caeeca9dc86cbc0f494d89c43aab4e Hash76
7835c1a2a0cb7249c82c9d283526188d Hash78
D:\Projects\Elance\AppinSecurityGroup\FtpBackup\Release\Backup.pdb
1c038adb34bd12940fc91d956eda0f85 Hash80
c95be0d57d7688861d685966069c18a2 Hash82
a6a9abbc67cbe071d6ed639fec3e1b84 Hash102
appinclient, Version 1.0
72a0da9442e1669e832c128936774c92 Hash109
e3ed385d2ce873eabe647c1c6de144eb Hash83
46110a31e7c579285ff9c2339c8e9dbf Hash85
8046761d8e617dc2dbbc3bc93fc91ed3 Hash86
17d0705bcc65eb16f6c8aee6cc0c384f Hash88
@*\AC:\New Folder\ba\New Folder\Backup\Backup\Downloader\HTTP downloader\New Folder\Project1.vbp
f8ecfee30bda0ad37f69f407f9a4c781 Hash89
8658145bdc3f0cae5357d4115b05543b Hash103
91f2bb5f6c2f3452724f831373474865 Hash98
f2a46ad687356eb9099bc7269411f76a Hash92
22d559800aa213a7150fa8b2e54b2b21 Hash95
9a9dc1bebfb0f6a713c5119f8c1b89a0 Hash96
@*\AC:\Http downloader(fud)\Project1.vbp
f6f131beb246d0c7f916c5c995ad91cd Hash100
cdc425240cb1e38c8432501062ff704a Hash101
6588efd38e17d44e3ff1ab91afd0f2b2 Hash105
f61db022aa5dfb59dbd53938c5a72a2c Hash110
62cddd629043f07a7f2ec3bdbc825ff9 Hash107
9b98e06c25c1ae3e8d0625b15a31fc75 Hash111
c43f52ec6902b9ee2be435072a9d3b2a Hash112
c14f235e08f6d855f5e73661fa758ff2 Hash75
c:\temp\elance\appinbot\Build\Win32\Release\appinclient.pdb
6fc6214a9cc6bb1ed442beda98fe47e6 Hash77
6b683fccfb118eb96af0cb8cfcc3b2f7 Hash79
9bf5982f68023900b678cfe08b76498e Hash84
C:\Users\PRED@TOR\Desktop\MODIFIED PROJECT LAB\FtpBackup(source code)\FtpBackup\Release\Backup.pdb
849fda2210df92da8d6d45f692a583b0 Hash87
B*\AD:\SOFTs\PRO\MY\SocketUploader\Copy of SocketSC\file_upload.vbp
e7c72900ede1a3fcebc40e72163642d3 Hash90
87f9beffa5b6198e5906efd971475dea Hash91
1e33463abb80297907d2de0ddad75a94 Hash99
e7c72900ede1a3fcebc40e72163642d3 Hash104
af41aaa36b787c95c0132551555dc8e1 Hash93
a1d78a37d6f278e99e0a904471cd448c Hash94
a810399062152e79c0f1d5e6b0f8c1ea Hash97
903b160fc4e720ea884e4222b5dc3f7e Hash106
21b11f60bfd420475d81726587310204 Hash108
D:\new versions\FTPUPLOADER\FTPUPLOADER_NK_1\FtpBackup_source\Release\Backup.pdb

C2 / Delivery Server *bluecreams[.]com* and Linked Malware Visualized

- **Phishing** – Hosted web pages for credential phishing. In many cases the same phishing pages were available through multiple target-named subdomains and URLs.
- **Lure Sites** – An interesting technique was the use of referenced “honeypots”. These sites would often be themed around a specific topic and lured the target to interact for credential phishing or malware delivery. One such example is `islam-jindabad.blogspot[.]com`, which remains online at the time of this writing. It was created in 2009 and referred to as a “honey pot” to Appin operators. The domain led to a second domain that delivered malware after clicking an image. The destination address of these images is `gmail-loginchk.freehostia[.]com/raj1.php`



18 SEPTEMBER 2009

Real Meaning Of Jihad For Muslim

In the Holy Quoran the book of Muslim Scriptures a question is posed, "what is the greates Jihad"? Many think the greatest Jihad is to fight evil around the world. Many think that it is waging war and killing people and blowing people like the way Osama Bin Laden and other Muslim Extremist have done. These terrorist often justify the killing of innocent people by saying they are waging war on the infidels. However this form of Jihad is nothing but a cheap excuse for terrorist to further their political and social causes.

The real meaning of Jihad is one that is internal deep within the individual. If there is evil done in the world is because people choose to do evil deeds. That is why Jihad does not really mean waging a holy war againts others but rather cleansing ourselves from influences, thought that czuses us to act in that evil ways. Jihad is restraining ourselves from working evil deeds.

POSTED BY ONE ALLAH (ISLAM JINDABAD) AT 5:30:00 AM

REAL TRUTH!!!

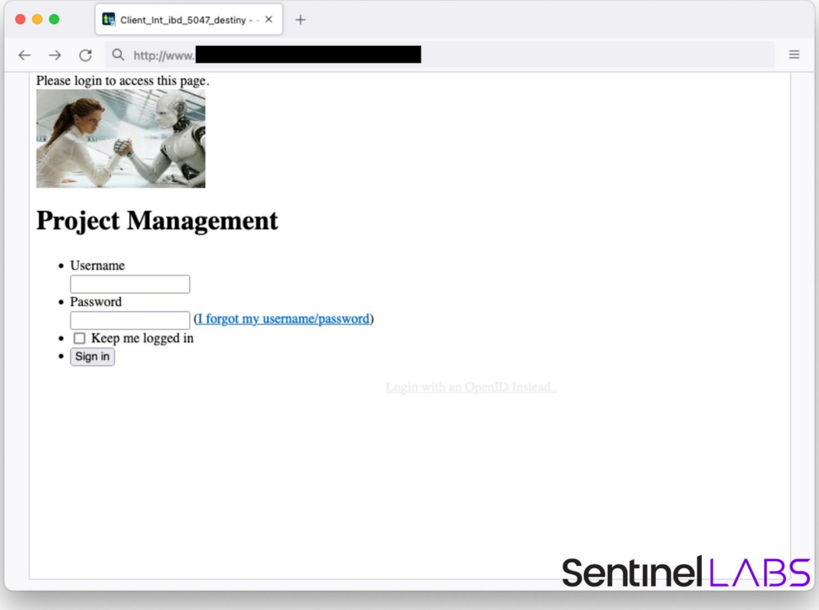
ROOT CAUSE OF JIHAD

MUMBAI TUMHARI JAAN

Malicious Lure Site, Directs to Malware Download

- **VPS Server** – Generic multi-purpose server for non-attributable access to victim machines and attack infrastructure administration. Typically accessed through SSH.

Additionally, a non-standard server type was also used by Appin covert communications. The business made use of specific websites for customer project tracking and data sharing. This was variously referred to as GoldenEye, Commando, or MyCommando, and acted as a place where customers could log in to view and download campaign specific data and status updates, communicate securely, and manage other aspects of their projects.



[redacted]

Please login to access this page.

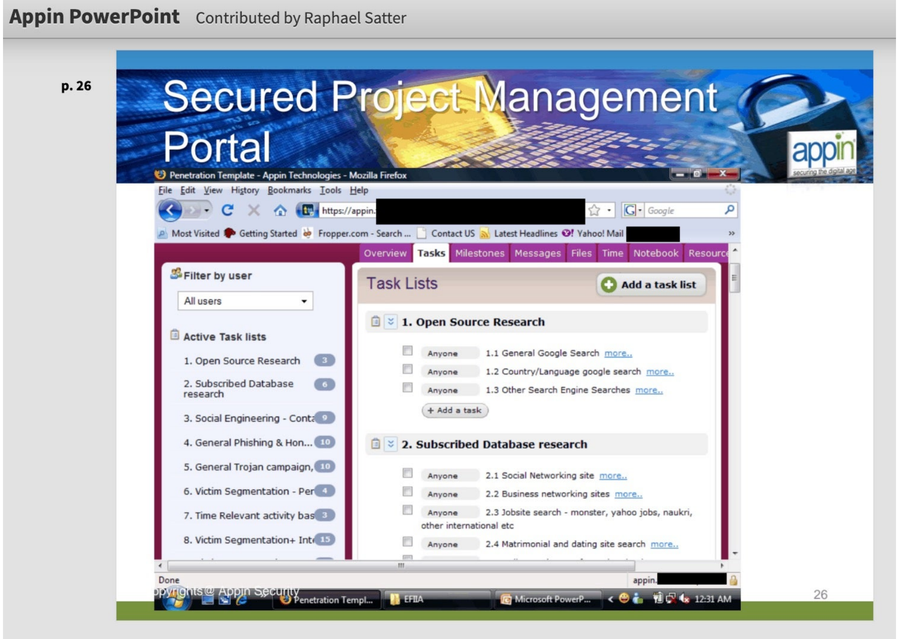
Project Management

- Username
- Password (I forgot my username/password)
- ☐ Keep me logged in
- Sign in

Login with an OpenID Instead...

Covert Communications Login

This is the same “Secured Project Management Portal” highlighted in an Appin marketing presentation, first shared by Reuters in their June 2022 mercenary hacker investigative report.



Appin PowerPoint Contributed by Raphael Satter

p. 26

Secured Project Management Portal

Penetration Template - Appin Technologies - Mozilla Firefox

File Edit View History Bookmarks Tools Help
https://appin.[redacted]
Google
Most Visited Getting Started Fropper.com - Search ... Contact US Latest Headlines Yahoo! Mail [redacted]
Overview
Tasks
Milestones
Messages
Files
Time
Notebook
Resourc

Filter by user

All users

Active Task lists

1. Open Source Research 3
2. Subscribed Database research 6
3. Social Engineering - Conta 9
4. General Phishing & Hon... 10
5. General Trojan campaign, 10
6. Victim Segmentation - Per 4
7. Time Relevant activity bas 3
8. Victim Segmentation+ Int 15

Task Lists

Add a task list

1. Open Source Research

□ Anyone 1.1 General Google Search more..
□ Anyone 1.2 Country/Language google search more..
□ Anyone 1.3 Other Search Engine Searches more..

+ Add a task

2. Subscribed Database research

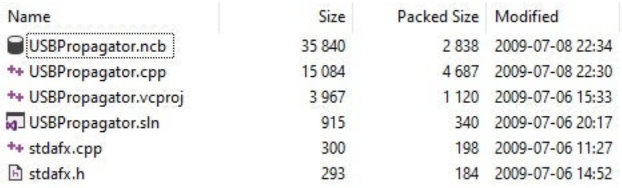
□ Anyone 2.1 Social Networking site more..
□ Anyone 2.2 Business networking sites more..
□ Anyone 2.3 Jobsite search - monster, yahoo jobs, naukri, other international etc
□ Anyone 2.4 Matrimonial and dating site search more..

Appin Marketing Document Showing Covert Communications Portal

Malware and Exploit Development

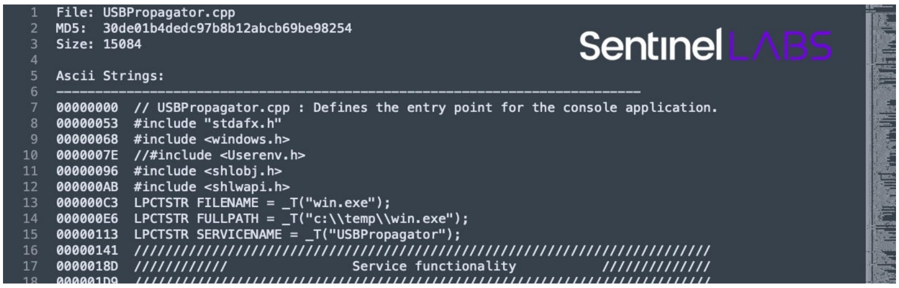
Appin made use of the California-based freelancing platform Elance (now known as Upwork) to purchase malware from external software developers, while also using internal employees to develop those projects and their own tools. Elance jobs were posted by Appin under the username “appinsecuritygroup”, and a profile set with the full name and `appinonline[.]com` email address of an Appin executive.

An example of Elance use is the purchase of the USB Propagator tool from the freelancer “alexstinger”. The original job posting was titled “Creation of Advanced Data Backup Utility”. The same tool is also referenced in the Operation Hangover report. The original version was purchased in 2009, for $500, after troubleshooting and source code delivery. The Elance job statement was completed on July 15th, 2009.



Name	Size	Packed Size	Modified
USBPropagator.ncb	35 840	2 838	2009-07-08 22:34
USBPropagator.cpp	15 084	4 687	2009-07-08 22:30
USBPropagator.vcproj	3 967	1 120	2009-07-06 15:33
USBPropagator.sln	915	340	2009-07-06 20:17
stdafx.cpp	300	198	2009-07-06 11:27
stdafx.h	293	184	2009-07-06 14:52

Source files delivered by “alexstinger”



```
File: USBPropagator.cpp
MD5:  30de01b4dedc97b8b12abcb69be98254
Size: 15084

Ascii Strings:
---------------------------------------------------------------------------
00000000  // USBPropagator.cpp : Defines the entry point for the console application.
00000053  #include "stdafx.h"
00000068  #include <windows.h>
0000007E  //#include <Userenv.h>
00000096  #include <shlobj.h>
000000AB  #include <shlwapi.h>
000000C3  LPCTSTR FILENAME = _T("win.exe");
000000E6  LPCTSTR FULLPATH = _T("c:\\temp\\win.exe");
00000113  LPCTSTR SERVICENAME = _T("USBPropagator");
00000141  ////////////////////////////////////////////////////////////////////////////
0000018D  ////////////                Service functionality              //////////////
000001D9  ////////////////////////////////////////////////////////////////////////////
```

Snapshot of source code delivered by “alexstinger”

Appin advertised on Elance for many other software projects as well, including ones titled:

- Audio Recording Software on Windows
- Creation of a code obfuscator for C, Visual C++
- Exploits for research purpose on MS Office and IE
- MS Office Exploits to upgrade our IPS/Antivirus!
- R&D in vulnerability research in Eastern Europe

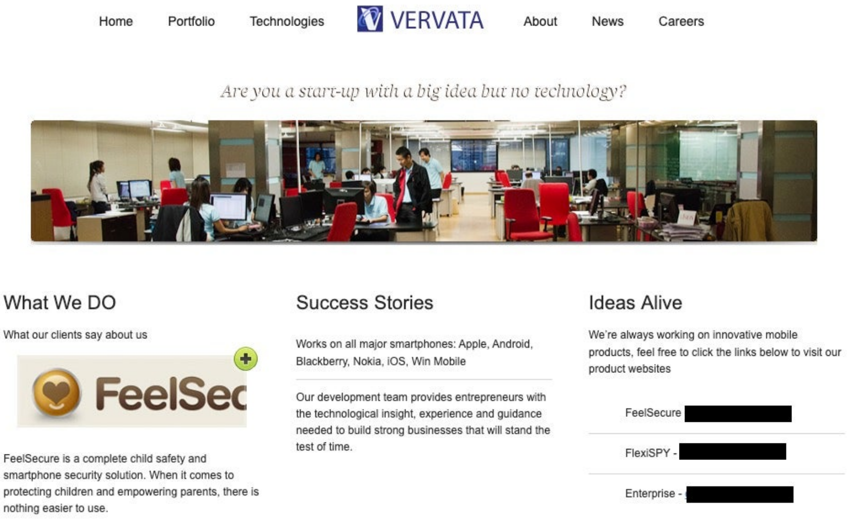
A summary of the job post for “R&D in vulnerability research in Eastern Europe” shows the following.

Description	To outsource research in exploits and vulnerabilities on a monthly retainer basis to expert organization in Eastern Europe
Skills Required	Vulnerability and Exploits Gathering, Exploit Development

Focus/Deliverables	Development of exploits on existing vulnerabilities or customization of exploit samples on the internet related to MS Office (Word, Excel, PowerPoint 2007/2003 etc), Adobe PDF, Browsers IE 6/7, Mozilla Firefox, Opera.
Minimum Expectation	At least two exploits a month, Exploits should be customizable with payloads, Minimum detection from AV, Weekly report on successes / failures.
Payment	$1,000 monthly

A recurring problem with these job postings was that freelancers quickly rejected them after noting the low payment amount and questioning whether they were intended for malicious use.

Appin made use of a large amount of private spyware and exploit services over the years, too. For example, in 2010 they purchased mobile spyware services through Vervata, the business behind the FlexiSPY mobile stalkerware. When this transaction was conducted, the domain `mobilebackup[.]biz` was used by operators for install guides, software downloads, and reviewing victim mobile device data. While this is historical data, it remains the case that FlexiSPY stalkerware is still marketed and sold today.



Are you a start-up with a big idea but no technology?

What We DO

What our clients say about us

FeelSecure is a complete child safety and smartphone security solution. When it comes to protecting children and empowering parents, there is nothing easier to use.

Success Stories

Works on all major smartphones: Apple, Android, Blackberry, Nokia, iOS, Win Mobile

Our development team provides entrepreneurs with the technological insight, experience and guidance needed to build strong businesses that will stand the test of time.

Ideas Alive

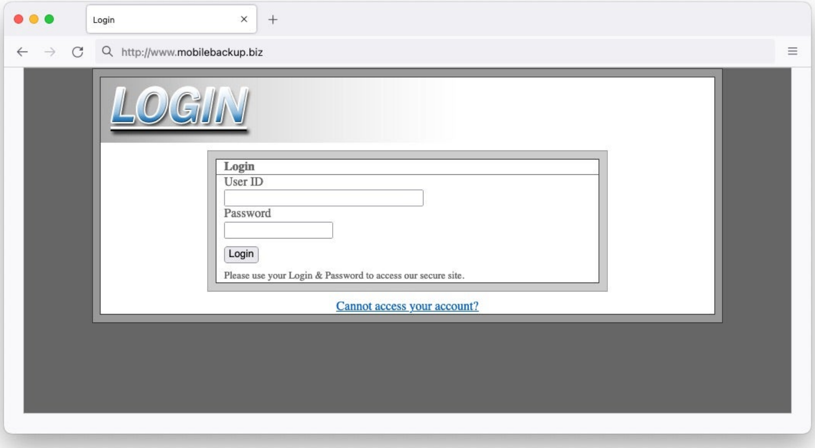
We're always working on innovative mobile products, feel free to click the links below to visit our product websites

FeelSecure [redacted]

FlexiSPY - [redacted]

Enterprise - [redacted]

Archived snapshot of Vervata homepage, FlexiSPY product offering at the time



Login

User ID

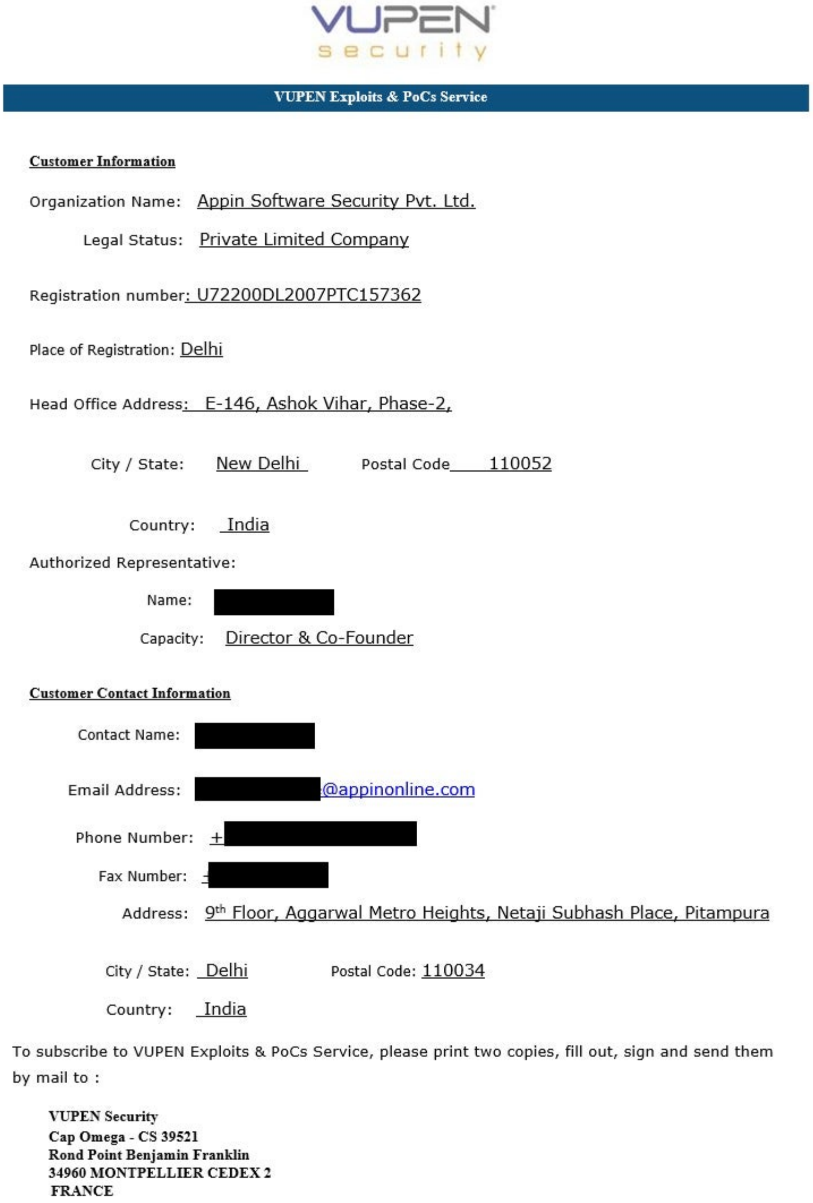
Password

Please use your Login & Password to access our secure site.

Cannot access your account?

Archived Flexispy Login Portal 2010

Appin later pursued the purchase of exploits from leading private vendors at the time, including Vupen and Core Security. Business interests also involved the opportunity for Appin to act as an exploit reseller for Vupen to the Indian Government.



VUPEN Exploits & PoCs Service

Customer Information

Organization Name: Appin Software Security Pvt. Ltd.

Legal Status: Private Limited Company

Registration number: U72200DL2007PTC157362

Place of Registration: Delhi

Head Office Address: E-146, Ashok Vihar, Phase-2,

City / State: New Delhi Postal Code 110052

Country: India

Authorized Representative:

Name: [redacted]

Capacity: Director & Co-Founder

Customer Contact Information

Contact Name: [redacted]

Email Address: [redacted]@appinonline.com

Phone Number: +[redacted]

Fax Number: +[redacted]

Address: 9th Floor, Aggarwal Metro Heights, Netaji Subhash Place, Pitampura

City / State: Delhi Postal Code: 110034

Country: India

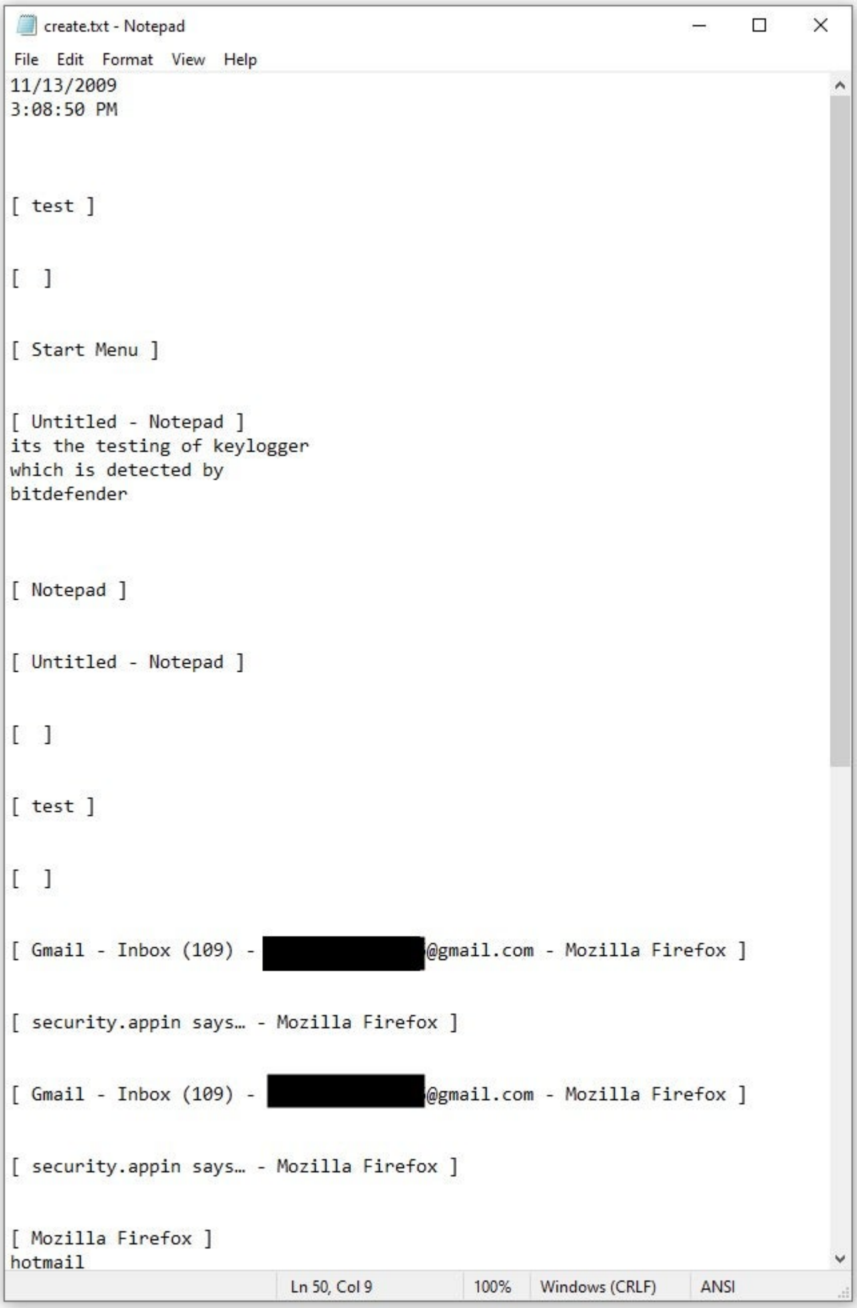
To subscribe to VUPEN Exploits & PoCs Service, please print two copies, fill out, sign and send them by mail to :

VUPEN Security
Cap Omega - CS 39521
Rond Point Benjamin Franklin
34960 MONTPELLIER CEDEX 2
FRANCE

Vupen and Appin Exploit Subscription Agreement Document

As noted, some malware was developed internally, including a keylogger. Associated data and communications reveal the initial intention of an employee first sharing their development of the keylogger to Appin leadership in August 2009. In a reviewed message, the employee noted a new keylogger being built which has the ability to upload logs to the FTP server.

Over the following weeks and months, tests were conducted to showcase the keylogger's capabilities. Here is one such file in which the developer tested the keylogger's functionality, being detected by third party antivirus solutions. Data redacted included the developer's personal email address.



```
11/13/2009
3:08:50 PM



[ test ]


[  ]


[ Start Menu ]


[ Untitled - Notepad ]
its the testing of keylogger
which is detected by
bitdefender



[ Notepad ]


[ Untitled - Notepad ]


[  ]


[ test ]


[  ]


[ Gmail - Inbox (109) - [redacted]@gmail.com - Mozilla Firefox ]


[ security.appin says… - Mozilla Firefox ]


[ Gmail - Inbox (109) - [redacted]@gmail.com - Mozilla Firefox ]


[ security.appin says… - Mozilla Firefox ]


[ Mozilla Firefox ]
hotmail
```

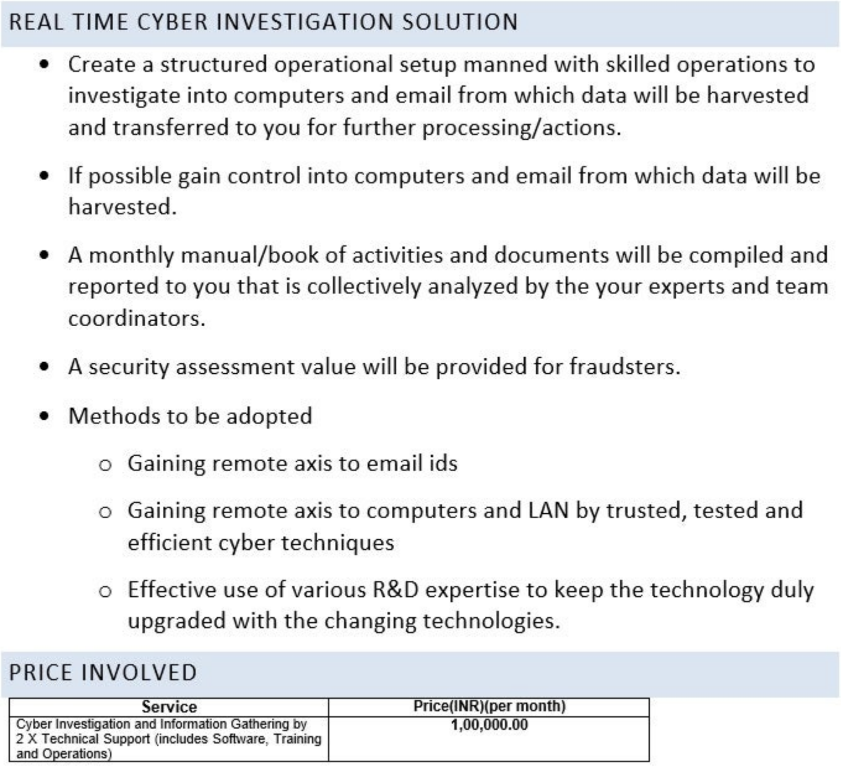
Keylogger Beaconing, Detected by AV

Months later the keylogger was being used in live operations, including in a campaign targeting the Pakistan government. Government victim data included personal email addresses and instant messaging activity, browsing for new jobs in the Pakistan Navy, reading/printing ISPR news, and other personally sensitive online activity.

The Hack-For-Hire Business

Although hack-for-hire organizations in India and elsewhere have evolved markedly over the years as both the technology available to them and the ecosystem in which they operate have changed, a clear snapshot of Appin's activity starting from around the early 2000's provides invaluable insight into the inner workings of such businesses.

Ignoring Appin's many business offerings related to network penetration testing, website security auditing, training and more, we can focus on the part most interesting to cyber defenders and threat intelligence analysts: the hack-for-hire offerings. Below is a proposed offering of Appin's 'Special Services Division' made to India's Chhattisgarh Police Cyber Investigation Cell.



REAL TIME CYBER INVESTIGATION SOLUTION

- Create a structured operational setup manned with skilled operations to investigate into computers and email from which data will be harvested and transferred to you for further processing/actions.
- If possible gain control into computers and email from which data will be harvested.
- A monthly manual/book of activities and documents will be compiled and reported to you that is collectively analyzed by the your experts and team coordinators.
- A security assessment value will be provided for fraudsters.
- Methods to be adopted
  - Gaining remote axis to email ids
  - Gaining remote axis to computers and LAN by trusted, tested and efficient cyber techniques
  - Effective use of various R&D expertise to keep the technology duly upgraded with the changing technologies.

PRICE INVOLVED

Service	Price(INR)(per month)
Cyber Investigation and Information Gathering by 2 X Technical Support (includes Software, Training and Operations)	1,00,000.00

Appin Special Services Division Offering (original text)

While a full review of the business structure is outside the scope of this report, a few relevant cybersecurity observations are useful to list:

- Offensive security services provided to customers, well over a decade ago, included data theft across many forms of technology, often internally referred to as “interception” services. These included keylogging, account credential phishing, website defacement, and SEO manipulation/disinformation. They would also accommodate other technical requests from a customer on-demand, such as cracking passwords from stolen documents.
- Operations Security (OPSEC) is taken seriously in theory, but was inadequately executed in practice. Operators, developers, and leadership were disciplined to not discuss project specifics (targets, customers, tools, etc.) through weak communication channels. However, it appears that leadership repeatedly initiated the failure to abide by those standards. Examples of this include analysts refusing to write down confidential technical information related to sensitive operations, while leadership openly discussed and documented the same details.
- The roles of individual operators are often built uniquely around their skill sets, rather than formal responsibilities based on a structured role. This includes operators and developers mixing tasks depending on the individual’s interests and career tenacity.
- There is a strong, financially incentivised push from leadership to all individual operators and developers for innovative ideas that can better achieve success on behalf of their customers. This includes finding new tools and techniques to accomplish the desire of the customer. Some OPSEC gaps originate from the resulting unchecked innovation.

A Day in the Life

While the operator and developer roles proved fluid over time, we can glimpse the leadership’s priorities based on weekly task lists handed down to the early ‘development’ group. Tasks were assigned to individuals, including the following objectives:

1) Individual A:

- Build fully functional & undetectable malicious documents using exploits.
- Resolve issues of malware not collecting specific messaging software logs.
- Coordinate with exploit developers (internal) for other ongoing campaigns.

2) Individual B:

- Build and finish the new network lateral movement solution.
- Rebuild “FTP Backup trojan” to make it fully undetectable.

3) Individual C:

- Build a new process with exploit developers (internal) for weekly use of new fully-undetectable attack tools.
- Troubleshoot phishing website problems, such as specific language characters not recording properly.

- Educate operators on other internal tools.

It’s ultimately unsurprising to learn of tasks and the individuals assigned to them; however, it is useful when contextualizing the overlapping technical links and improvements between campaigns, such as version updates of the FTP Backup trojan.

Moving Forward

Our examination of the Indian hack-for-hire group Appin underscores the enduring and substantial threat posed by such entities to businesses, governments, and individuals over an extended period exceeding a decade. The research findings underscore the group’s remarkable tenacity and a proven track record of successfully executing attacks on behalf of a diverse clientele. The technical insights and infrastructure provided by our study offer a valuable resource for mapping associated malicious activities and reevaluating past incidents with a renewed perspective.

The concerning resilience of these groups, coupled with their capacity to attract new clients despite heightened public scrutiny, emphasizes the urgent necessity for enhanced international cooperation and the establishment of robust legal frameworks to effectively address this escalating challenge. In light of advancing technologies and a growing demand for digital espionage and cybercrime services, it is imperative for governments, businesses, and high-risk individuals to proactively implement measures to protect themselves against these formidable, adaptable, and thriving hack-for-hire threat actors.

Historical Indicators of Compromise

Note, some of the following indicators have since been used for legitimate reasons or sinkholed. Therefore, we advise caution if considering these as active indicators in their current state.

IPs
64.186.132[.]165
65.75.243[.]251
65.75.250[.]66
69.197.147[.]146
75.127.111[.]165
75.127.78[.]100
75.127.91[.]16
84.243.201[.]254
212.72.189[.]74

Domains
abdupdates[.]com
alr3ady[.]net
antivirusreviewratings[.]com
authorisedsecurehost[.]com
bksrv3r001[.]com
bluecreams[.]com
bookshopmarket[.]com
brandsons[.]net
braninfall[.]net
c00lh0sting[.]com
c0ttenc0unty[.]com
cr3ator01[.]net
crowcatcher[.]com
crvhostia[.]net
currentnewsstore[.]com
customauthentication[.]com
devinmartin[.]net
directsupp0rt[.]com
divinepower[.]info
draganheart[.]com
easyhost-ing[.]com
easyslidesharing[.]net
f00dlover[.]info
filetrusty[.]net
follow-ship[.]com
forest-fire[.]net
foxypredators[.]com
freensecurehost[.]com
freesecurehostings[.]com
freewebdomainhost[.]com

freewebuserhost[.]com
gauzpie[.]com
gmail-loginchk[.]freehostia[.]com
h3helnsupp0ort[.]com
hatemewhy[.]com
hostingserveronline[.]net
hotmasalanewssite[.]com
islam-jindabad[.]blogspot[.]com
jasminjorden[.]]com
jasminjorden[.]com
karzontheway[.]com
kungfu-panda[.]info
matrixnotloaded[.]com
msfileshare[.]net
msoftweb[.]com
myt3mple[.]com
newamazingfacts[.]com
nitr0rac3[.]com
pc-technsupport[.]com
piegauz[.]net
r3gistration[.]net
reliablensecurehost[.]net
s0pp0rtdesk[.]com
s3rv1c3s[.]net
secuina[.]net
securenhost[.]com
server003[.]com
server006[.]com
serverrr[.]com
serviceaccountloginservicemail[.]info
servicesaccount[.]com
sliderocket[.]com
speedaccelator[.]com
spidercom[.]info
t3rmin3[.]com
taraanasongs[.]com
thedailynewsheadline[.]com
tow3r[.]info
updatemypc[.]net
updatesl1nk[.]com
vall3y[.]com
wearwellgarments[.]eu
webjavaupdate[.]com
webmicrosoftupdate[.]net

Files SHA1

02e6ddbc715dfd7ce1838c4b4b0520c8
03636f6d4f0041859f009893eac67690
055ce289ee5d2c74e3a4de967f0ff82c
0936b73c4a0acae8fe9517e26536c058
0948c7444ff919ec7218ad04c29c8189
0a8435a4abe99c22b8e1a1673098821a
0aa0116bcfcf1da87af0ec393e2b8061
0c68acbe505877eee81aaaefd6be5d57
0cd662b540c642ac9a6972226a2ee8ae
0f65c1202881f5c0e3d512aa64162716
0f6e7efe4630bf314fd5d895f55bcd08
1782314da3da2f4fdcbda269ddfa7830
17d0705bcc65eb16f6c8aee6cc0c384f
182b4f223a20d10fa39a8577a7b285f8
186f71e7db3188347f3c7e3608e40a76
1a708fb0d40f0f66e75afe26f0754f3c
1ad6ac5126fbf79d92e211e7459a04fd
1c038adb34bd12940fc91d956eda0f85
1e33463abb80297907d2de0ddad75a94
20aa596a83117d12faebda225f4dcf25
21609c45130fbba1a8c07b6fe864bbc4

```
21b11f60bfd420475d81726587310204
22d559800aa213a7150fa8b2e54b2b21
2546f1229ddf1a45ab944a8a0da642ca
25472d552f3439d610a0ea0feea59b18
283b06e0931d58b320fb5222bd9e2327
28f7de0a63dd9f069e9892a7b9c1393e
2cf626da0f86b4ca0ce5ff12bbdd50b4
2fdb2e334bc32856898c4c5a9b7038bf
3625f274b26050e913d21280689580aa
3fa8a69d0e9f0163382d4733e7546061
40dc57f0e7eab28eac628cd7d58670f2
46110a31e7c579285ff9c2339c8e9dbf
463922075362745a02969f0cc34adb48
482840e161a8c5fb14fe57d13c7e58b1
48d0bca6196781e4030d2427e0cebb7c
4a4392583dd001c3729f8705e62f06d0
4ac3a570f006a1b0e016257d3be5018c
4d4c8e85691295de8552aab888979026
4ebe9891f10e93cbd18266b36f1b6e6e
51c984dac039092447879d40164fc949
572fb7ba509d5b2a57142149d6fb0dd7
596d1f7a84729cfb608b29f687ce318b
5b0172d4f6b3970cc460cbe0556b6466
5dddb3f57c9066b6d3d076f590d40d0a
5deabcd480ff2df5de3a93c081b76dda
5f04cf580b375ac90caf75930fd866e7
62cddd629043f07a7f2ec3bdbc825ff9
6588efd38e17d44e3ff1ab91afd0f2b2
672bb005aeaf5805c6d06c581a8d1b10
67caeeca9dc86cbc0f494d89c43aab4e
6b683fccfb118eb96af0cb8cfcc3b2f7
6cc8f81c50b8e86feea0dd800f3e8901
6cd6aa3065d51f3c14784b2abb87b2a4
6e6eb5af7488e5c9e1ada0efd624235f
6fc6214a9cc6bb1ed442beda98fe47e6
72a0da9442e1669e832c128936774c92
74e571f9accf9fe1b4ea6ee0e02a5180
75b61ceaf2dc1acce6de9c55103f7f05
77373d579ac6479adf7140340abeb667
77e88fa11cb0cf44c4691c04742d1b13
7835c1a2a0cb7249c82c9d283526188d
79b914e089fe7b1029dd38bb08d7dcd4
7a8c0735b6e631651a6618a789b86315
7baad0dba7909e810c55f4678c301d7e
8046761d8e617dc2dbbc3bc93fc91ed3
81c33d5c2d1d71d2639283be169ad235
82262bf6215659485d31df672562060d
849fda2210df92da8d6d45f692a583b0
862f6fe18ff2f493a8b3b927d51e82b3
8658145bdc3f0cae5357d4115b05543b
87f05d07b1c60b317d3fb60335745428
87f9beffa5b6198e5906efd971475dea
8a65479b077295d8420430e9f114b6a2
8ca0082df24a060c0edcd3a4875a63ab
903b160fc4e720ea884e4222b5dc3f7e
91c21e837620a005c8d5e1cb73e9bfb8
91f2bb5f6c2f3452724f831373474865
9225fc6926516f04bf87e44b3e9201e1
92bfb44848a886b388576c60745aa605
963fbcdaec66a5fcd5664e932fa06f4d
9a9dc1bebfb0f6a713c5119f8c1b89a0
9b98e06c25c1ae3e8d0625b15a31fc75
9bf5982f68023900b678cfe08b76498e
a053b31eaa11e2eedc0182a8e0051bf3
a1d78a37d6f278e99e0a904471cd448c
a33175880547ab5296c302681290c922
a3ecdcf43f89074e4042d01987255a5f
```

```
a5d3738287ec9d74ca9bcdd5fa2d9018
a6a9abbc67cbe071d6ed639fec3e1b84
a810399062152e79c0f1d5e6b0f8c1ea
aa026aaa783f691c6da7c286af5439c7
aa8039e7b0c08c369820f450f2a12ef8
ad6cc39b31878c270bf1f4e106c1f773
ae03020fc96296a210d26e9efa0948c6
af41aaa36b787c95c0132551555dc8e1
af7ed912b633fcad5d4e9b52df9de72a
b35702471ac848a23b33b4b3aaaddf04
b3ec88a92a5881e10f6dd46a2e43f419
b5724f5b127e118babbbd4f31f93da7b
b5a53dfa9a2b5bdae9f5bd99b114cf75
b5d248e62a6c593d19104411b411146f
b6a371b2dc3143e3c5df0abc2c0604a3
b7b6dd5bcb3dcd87b74d1485b356a560
b7d18dbe6cad4b54b588ec5eed3a8141
b86fd1cfe2de2ea841f8f522dee6370c
b8baedf06d212a1769c17741a22dbabb
bba2d1e279101d9df3ee135a997457c7
bba7accf299c87080a7c12f3913b851a
bc04127266eab3c142fd9ab8bf16cae2
be4fcca6b05fcd65ca2d8e42c1f7f685
c14f235e08f6d855f5e73661fa758ff2
c4130bcfbec35b377b512ceb64221293
c43f52ec6902b9ee2be435072a9d3b2a
c44e2798f7a6a18b7a61d811bd884981
c48e5210cf6fb3286f8bc66106456686
c5a9f8a833d8eafa50d81f04fed7d42a
c7cb3ec000ac99da19d46e008fd2cb73
c8717112454bb0bee2d8afcba4c55c31
c95be0d57d7688861d685966069c18a2
cb3a7c4433e35ff3dfede853731c5004
cd6e61b12e08cab7f5a6201c6db5d6bd
cdc425240cb1e38c8432501062ff704a
ce157212cd908bc0d3b16949822dec6f
d0e966b61e15490ad958b8db3a4a624b
d2a1dc1cde78900927bd6a0ffc3a87a2
d6821dcf113e28e2c852febf5d0f2725
d8dcf2a53505a61b5915f7a1d7440a2e
daf3f0ed5e86cb7c0f6553911051c39e
ddef9714a67219b45eb0e6f66a447c11
de50630da67f860a402d5bd298f5224f
e3ed385d2ce873eabe647c1c6de144eb
e6b37e2113471b4b7acc833c99fc9c0f
e7c72900ede1a3fcebc40e72163642d3
e952bba9789b7e2983d2441ba52d9a19
ecac2ce6e52c78718c0d0f7a99829136
ed67f4e36aabf56d8fb830463cbc5487
eddd399d3a1e3a55b97665104c83143b
ef3b0ae4d6870291f6812ed77e23b558
f0dba8a8349552e5e632d395cd1be8ea
f2036ae83a79f62c749913576ba63ba6
f211694aaf443b12b2eca9f5e7f25407
f2a46ad687356eb9099bc7269411f76a
f4949579248c94ee81ed1a6a8c246126
f61db022aa5dfb59dbd53938c5a72a2c
f6f131beb246d0c7f916c5c995ad91cd
f8df4e8457d1c6f4f395701b0f9e839b
f8ecfee30bda0ad37f69f407f9a4c781
f9cdf5bebdee5486d26cd0e1a6c3d336
fad0db73af342501a0568730b4a24d79
fb72b395080807571cd784be89415612
fdfcb23f537d4265bab7f28ec9b9e036
```