ADVANCED PERSISTENT THREAT
(HTTPS://WWW.SENTINELONE.COM/LABS/CATEGORY/ADVANCED-PERSISTENT-THREAT/)

Transparent Tribe (APT36) | Pakistan-Aligned Threat Actor Expands Interest in Indian Education Sector

ALEKSANDAR MILENKOSKI (HTTPS://WWW.SENTINELONE.COM/BLOG/AUTHOR/ALEKSMIL/) /
APRIL 13, 2023 (HTTPS://WWW.SENTINELONE.COM/BLOG/2023/04/)

Executive Summary

- SentinelLabs has been tracking a cluster of malicious documents that stage Crimson RAT, distributed by APT36 (Transparent Tribe).
- We assess that this activity is part of the group's previously reported targeting of the education sector in the Indian subcontinent.
- We observed APT36 introducing OLE embedding to its typically used techniques for staging malware from lure documents and versioned changes to the

Overview

SentinelLabs has been tracking a recently (https://twitter.com/StopMalvertisin/status/1640798678649827329) disclosed cluster of malicious Office documents that distribute Crimson RAT, used by the APT36 group (also known as Transparent Tribe) targeting the education sector. This post summarizes our observations highlighting the group's continuous change in used malware staging techniques and Crimson RAT implementations.

Transparent Tribe (https://attack.mitre.org/groups/G0134/) is a suspected Pakistan-based threat group active since at least 2013. The group is not very sophisticated; however, it is a highly persistent threat actor that continuously adapts its operational strategy. Transparent Tribe has previously focused mainly on Indian military and government personnel, but it has recently expanded its scope to include educational institutions and students in the Indian subcontinent. Crimson RAT is a consistent staple in the group's malware arsenal the adversary uses in its campaigns.

The names and content of the lure documents, the associated domains, and the use of Crimson RAT suggest that the activities discussed in this post are part of a previously reported (https://blog.talosintelligence.com/transparent-tribe-targets-education/) broader targeting of the education sector by Transparent Tribe.

Further, the PDB paths of some Crimson RAT samples we analyzed contain the word `Wibemax`, which is also contained in the PDB paths of Crimson RAT payloads observed in a previous (https://community.fortinet.com/t5/FortiEDR/Threat-Coverage-How-FortiEDR-protects-against-CrimsonRAT/ta-p/215398) Transparent Tribe campaign.

Wibemax matches the name of a Pakistani software development company, but at this time we have not identified a clear relationship to the adversary.

It is worth noting that there are high confidence assessments (https://blog.talosintelligence.com/transparent-tribe-targets-education/) of Transparent Tribe leveraging third parties to support their operation, such as the Pakistani web

crucial role this activity plays in fulfilling the goals and aspirations of the authorities whose interests Transparent Tribe represents.

Malicious Documents

The documents that Transparent Tribe distributes have education-themed content and names such as assignment (https://www.virustotal.com/gui/search/name%253Aassignment.docx) or `Assignment-no-10`, and indicate creation dates of July and August 2022. Based on known behavior of this group, we suspect that the documents have been distributed to targets as attachments to phishing emails. Consistent with known Transparent Tribe tactics, we observed that some of the documents have been hosted on file hosting services and attacker-created domains, such as `s1.fileditch[.]ch`, `cloud-drive[.]store`, and `drive-phone[.]online`.

It is important to note that `cloud-drive[.]store` and `drive-phone[.]online` have been previously linked (https://blog.talosintelligence.com/transparent-tribe-targets-education/) to Transparent Tribe activities targeting the education sector and assessed as domains prepared for future use. Further, `drive-phone[.]online` closely resembles the `phone-drive[.]online` domain recently observed (https://www.welivesecurity.com/2023/03/07/love-scam-espionage-transparent-tribe-lures-indian-pakistani-officials/) hosting Transparent Tribe malware targeting Indian and Pakistani Android users.

The malicious documents we analyzed stage Crimson RAT using Microsoft Office macros or OLE embedding.

The macro code executes when the documents are opened, and its functionality is consistent with known Transparent Tribe macro variants. The macros create and decompress an embedded archive file in the `%ALLUSERSPROFILE%` directory (`C:\ProgramData`) and execute the Crimson RAT payload within. Some macros insert text in the document, which is typically education-themed content relating to India.

```
    file_nameLilliypatel = "Witchher"
    fldr_nameLilliypatel = Environ$("ALLUSERSPROFILE") & "\PoEc\"

    If Dir(fldr_nameLilliypatel, vbDirectory) = "" Then
        MkDir (fldr_nameLilliypatel)
    End If
    [...]
    If vnLilliypatel >= v8 Then

       [...]

        Open path_fileLilliypatel & ".zip" For Binary Access Write As #2
            Put #2, , btsSocdaLilliypatel8
        Close #2
        fvLilliypatel = fvLilliypatel & ".e"
     End If
    [...]
    If Dir(fvLilliypatel & "xe") = "" Then
        umahznip fldr_nameLilliypatel & file_nameLilliypatel & ".zip", fldr_nameLilliypatel
    End If
    Shell fvLilliypatel & "xe", 1
    Call docLdrLilliypatel
End Sub
```

Macro implementation

```
UNIT 1: Origin of Earth and System processes
Solar system formation and planetary differentiation; formation of the Earth: formation
and composition of core, mantle, crust; chemical composition of Earth; geological time scale and
major changes on the Earth's surface; Holocene and the emergence of humans. Concept of plate
tectonics and continental drift theory, continental collision and formation of the Himalaya; ocean
floor spreading; mantle convection and, major plates; earthquakes; volcanic activities; orogeny;
isostasy; gravitational and magnetic fields of the earth; paleontological evidences of plate
tectonics.

[...]

UNIT 4: Importance of being a mountain
Formation of Peninsular Indian mountain systems - Western and Eastern Ghats,
Vindhyas, Aravallis, etc. Formation of the Himalaya; development of glaciers, perennial river
systems and evolution of monsoon in Indian subcontinent; formation of Indo-Gangetic Plains,
arrival of humans; evolution of Indus Valley civilization; progression of agriculture in the Indian
subcontinent in Holocene; withdrawing monsoon and lessons to draw.
```

Macro-inserted document text

In addition to macros, we observed that Transparent Tribe have adopted OLE embedding as a technique to stage Crimson RAT. Malicious documents that implement this technique require users to double-click a document element. The documents distributed by Transparent Tribe typically display an image (a “View Document” graphic) indicating that

The “View Document” graphic

```
EBDF 0300 0200 4D69 6372 6F73 6F66 7420  ëß....Microsoft
5570 6461 7465 2E65 7865 0043 3A5C 5573  Update.exe.C:\Us
6572 735C 576F 726B 5C44 6573 6B74 6F70  ers\Work\Desktop
5C64 6573 6B74 6F70 5C74 6774 2073 7973  \desktop\tgt sys
5C53 616C 6D61 6E5C 5375 6E6E 795C 3820  \Salman\Sunny\8
4A75 6C79 2032 325C 4D69 6372 6F73 6F66  July 22\Microsof
7420 5570 6461 7465 2E65 7865 0000 0003  t Update.exe....
0036 0000 0043 3A5C 5573 6572 735C 576F  .6...C:\Users\Wo
726B 5C41 7070 4461 7461 5C4C 6F63 616C  rk\AppData\Local
5C54 656D 705C 4D69 6372 6F73 6F66 7420  \Temp\Microsoft
5570 6461 7465 2E65 7865 0000 DE03 004D  Update.exe..Þ..M
5A90 0003 0000 0004 0000 00FF FF00 00B8  Z .........ÿÿ..¸
0000 0000 0000 0040 0000 0000 0000 0000  .......@........
0000 0000 0000 0000 0000 0000 0000 0000  ................
0000 0000 0000 0000 0000 0080 0000 000E  ...............€
1FBA 0E00 B409 CD21 B801 4CCD 2154 6869  .º..´.Í!¸.LÍ!Thi
7320 7072 6F67 7261 6D20 6361 6E6E 6F74  s program cannot
2062 6520 7275 6E20 696E 2044 4F53 206D   be run in DOS m
6F64 652E 0D0D 0A24 0000 0000 0000 0050  ode....$.......P
```

OLE stream that stores Crimson RAT

designated Crimson RAT loaders. The adoption of OLE embedding further highlights the group's continuous experimentation with malware staging techniques.

Crimson RAT Implementations

We observed a variety of Crimson RAT `.NET` implementations, with compilation timestamps between July and September 2022. The Crimson RAT payloads we analyzed use the `richa-sharma.ddns[.]net` domain for C2 purposes and support either 40 or 65 commands, most of which have been documented in previous (https://www.zscaler.de/blogs/security-research/targeted-attack-indian-financial-institution-delivers-crimson-rat) research (https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf). Features of Crimson RAT include exfiltrating system information, capturing screenshots, starting and stopping processes, and enumerating files and drives.

```
[...]
    if (!(text5 == "Toronto$cl0rklg"))
    {
        continue;
    }
    goto IL_D6B;
}
else
{
    if (!(text5 == "Toronto$au0dio"))
    {
        continue;
    }
    goto IL_E7B;
}
[...]
```

A Crimson RAT command dispatch routine

(https://community.fortinet.com/t5/FortiEDR/Threat-Coverage-How-FortiEDR-protects-against-CrimsonRAT/ta-p/215398) Transparent Tribe campaign, such as `D:\Projects\Wibemax\WinP\WinP\obj\Debug\WinP.pdb` and `D:\Projects\Wibemax\Windows RAT\1 Windows 10 Client\Win8P-Sunny\2022-04-15-Win8P Sunny\obj\Debug\FUJIKBattery.pdb`.

```
D:\Projects\Wibemax\Windows RAT\1 Windows 10 Client\Sunny\2022-06-17 Richa\W8P Sunny\obj\Debug\Kosovo.pdb
D:\Projects\Wibemax\Windows RAT\1 Windows 10 Client\Sunny\2022-06-17 Richa\W8P Sunny\obj\Debug\Toronto.pdb
```

Crimson RAT PDB paths

We observed different Crimson RAT version identifiers: `R.S.8.8.`, `R.S.8.9`, `R.S.8.1`, and `R.S.8.6`. We speculate that the `R.S.` components of the identifiers may relate to the configured C2 domain (`richa-sharma.ddns[.]net`) and the numerical components may specify a version (build) number. This aligns with a documented (https://labs.k7computing.com/index.php/transparent-tribe-targets-educational-institution/) Crimson RAT variant with the identifier `S.L.2.2.`, which has used the `sunnyleone.hopto[.]org` domain for C2 purposes.

As an anti-analysis measure, Crimson RAT variants delay their execution for a given time period, for example, 61, 180, or 241 seconds. Most of the Crimson RAT variants we analyzed evaluate whether they execute at a machine named `G551JW` or `DESKTOP-B83U7C5` and establish persistence by creating a registry key under `\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` only if the victim's machine name differs. `G551JW` or `DESKTOP-B83U7C5` may be the names of the machines where Crimson RAT developers have been running test executions.

Crimson RAT variants implement different obfuscation techniques of varying intensities, for example, simple function name malformation and dynamic string resolution. We observed the use of the Eazfuscator (https://www.gapotchenko.com/eazfuscator.net)

```
private static bool smethod_0(bool bool_0)
{
    DateTime dateTime = DateTime.Parse(Class27.smethod_0(-877831690),
    CultureInfo.InvariantCulture, DateTimeStyles.RoundtripKind);
    DateTime utcNow = DateTime.UtcNow;
    if (!(utcNow > dateTime) && !(utcNow < dateTime.AddDays(-21.0)))
    {
        return true;
    }
    string name = typeof(Class20).Assembly.GetName().Name;
    string.Format(Class27.smethod_0(-877831723), name);
    return true;
}
```

Eazfuscator trial period evaluation in *NewOrleans*

```
This copy of 'NewOrleans' has expired and will no longer run.

This happened because it was created using an evaluation version of Gapotchenko's Eazfuscator.NET
which is only licensed for testing purposes.

You should report this problem to the vendor of 'NewOrleans'.
```

Eazfuscator trial expiry message

With previous (https://labs.k7computing.com/index.php/transparent-tribe-targets-educational-institution/) variants of Crimson RAT obfuscated using Crypto Obfuscator (https://www.ssware.com/cryptoobfuscator/obfuscator-net.htm), the addition of Eazfuscator to the obfuscation techniques used by Transparent Tribe highlights the continuous maintenance and development of the RAT.

Conclusion

Transparent Tribe is a highly motivated and persistent threat actor that regularly updates its malware arsenal, operational playbook, and targets. Our analysis further demonstrates this characteristic of the group by spotlighting the adoption of OLE embedding as a technique for staging malware from lure documents and the Eazfuscator

Indicators of Compromise

SHA1	Description
738d31ceca78ffd053403d3b2bc15847682899a0	Malicious document
9ed39c6a3faab057e6c962f0b2aaab07728c5555	Malicious document
af6608755e2708335dc80961a9e634f870aecf3c	Malicious document
e000596ad65b2427d7af3313e5748c2e7f37fba7	Malicious document
fd46411b315beb36926877e4b021721fcd111d7a	Malicious document
516db7998e3bf46858352697c1f103ef456f2e8e	Crimson RAT
842f55579db786e46b20f7a7053861170e1c0c5e	Crimson RAT
87e0ea08713a746d53bef7fb04632bfcd6717fa9	Crimson RAT
911226d78918b303df5110704a8c8bb599bcd403	Crimson RAT
973cb3afc7eb47801ff5d2487d2734ada6b4056f	Crimson RAT

Domain	Description
richa-sharma.ddns[.]net	C2 server
cloud-drive[.]store	Malware hosting location
drive-phone[.]online	Malware hosting location
s1.fileditch[.]ch	Malware hosting location

APT (HTTPS://WWW.SENTINELONE.COM/BLOG/TAG/APT/)

PDF (https://www.sentinelone.com/wp-content/uploads/pdf-gen/1681348035/transparent-tribe-apt36-pakistan-aligned-threat-actor-expands-interest-in-indian-education-sector.pdf)

ALEKSANDAR MILENKOSKI
(https://www.sentinelone.com/blog/author/aleksmil/)

Aleksandar Milenkoski is a Senior Threat Researcher at SentinelLabs. With expertise in malware research and focus on targeted attacks, he brings a blend of practical and deep insights to the forefront of cyber threat intelligence. Aleksandar has a PhD in system security and is the author of numerous reports on cyberespionage and high-impact cybercriminal operations, conference talks, and peer-reviewed research papers. His research has won awards from SPEC, the Bavarian Foundation for Science, and the University of Würzburg.

(https://www.linkedin.com/in/aleksmilenkoski/) (https://twitter.com/milenkowski)

PREV

Dissecting AlienFox | The Cloud Spammer's Swiss Army Knife
(https://www.sentinelone.com/labs/dissecting-alienfox-the-cloud-spammers-swiss-army-knife/)

NEXT

Kimsuky Evolves Reconnaissance Capabilities in New Global Campaign
(https://www.sentinelone.com/labs/kimsuky-evolves-reconnaissance-capabilities-in-new-global-campaign/)

Embrace Lua
(https://www.sentinelone.com/labs/sandman-apt-china-based-adversaries-embrace-lua/)
DECEMBER 11 2023

Elephant Hunting | Inside an Indian Hack-For-Hire Group
(https://www.sentinelone.com/labs/elephant-hunting-inside-an-indian-hack-for-hire-group/)
NOVEMBER 16 2023

Arid Viper | APT's Nest of SpyC23 Malware Continues to Target Android Devices
(https://www.sentinelone.com/labs/arid-viper-apts-nest-of-spyc23-malware-continues-to-target-android-devices/)
NOVEMBER 06 2023

RECENT POSTS

(https://www.sentinelone.com/labs/exploring-fbot-python-based-malware-targeting-cloud-and-payment-services/)

Exploring FBot | Python-Based Malware Targeting Cloud and Payment Services (https://www.sentinelone.com/labs/exploring-fbot-python-based-malware-targeting-cloud-and-payment-services/)

January 11, 2024

(https://www.sentinelone.com/labs/labscon-replay-spectre-strikes-again-introducing-the-firmware-edition/)

LABScon Replay | Spectre Strikes Again: Introducing the Firmware Edition (https://www.sentinelone.com/labs/labscon-replay-spectre-strikes-again-introducing-the-firmware-edition/)

December 28, 2023

(https://www.sentinelone.com/labs/labscon-replay-intellexa-and-cytrox-from-fixer-upper-to-intel-agency-grade-spyware/)

LABSCon Replay | Intellexa and Cytrox: From Fixer-Upper to Intel Agency Grade Spyware (https://www.sentinelone.com/labs/labscon-replay-intellexa-and-cytrox-from-fixer-upper-to-intel-agency-grade-spyware/)

December 26, 2023

LABS CATEGORIES

Crimeware (https://www.sentinelone.com/labs/category/crimeware/)

Security Research (https://www.sentinelone.com/labs/category/security-research/)

Advanced Persistent Threat (https://www.sentinelone.com/labs/category/advanced-persistent-threat/)

Adversary (https://www.sentinelone.com/labs/category/adversary/)

LABScon (https://www.sentinelone.com/labs/category/labscon/)

Security & Intelligence (https://www.sentinelone.com/labs/category/security-intelligence/)

ıttps://twitter.com/LabsSentinel) in(https://www.linkedin.com/company/sentinelone)

LABS

(https://www.sentinelone.com/labs/)

SENTINELLABS

In the era of interconnectivity, when markets, geographies, and jurisdictions merge in the melting pot of the digital domain, the perils of the threat ecosystem become unparalleled. Crimeware families achieve an unparalleled level of technical sophistication, APT groups are competing in fully-fledged cyber warfare, while once decentralized and scattered threat actors are forming adamant alliances of operating as elite corporate espionage teams.

RECENT POSTS

Exploring FBot | Python-Based Malware Targeting Cloud and Payment Services (https://www.sentinelone.com/labs/exploring-fbot-python-based-malware-targeting-cloud-and-payment-services/)

JANUARY 11, 2024

(https://www.sentinelone.com/labs/exploring-fbot-python-based-malware-targeting-cloud-and-payment-services/)

LABScon Replay | Spectre Strikes Again: Introducing the Firmware Edition (https://www.sentinelone.com/labs/labscon-replay-spectre-strikes-again-introducing-the-firmware-edition/)

DECEMBER 28, 2023

(https://www.sentinelone.com/labs/labscon-replay-spectre-strikes-again-introducing-the-firmware-edition/)

ıttps://twitter.com/LabsSentinel) in(https://www.linkedin.com/company/sentinelone)

LABS

(https://www.sentinelone.com/labs/)

replay-
intellexa-
and-cytrox-
from-fixer-
upper-to-
intel-agency-
grade-
spyware/)

SIGN UP

Get notified when we post new content.

Business Email >

By clicking Subscribe, I agree to the use of my personal data in accordance with SentinelOne Privacy Policy (/legal/privacy-policy/). SentinelOne will not sell, trade, lease, or rent your personal data to third parties. This site is protected by reCAPTCHA and the Google Privacy Policy (https://policies.google.com/privacy) and Terms of Service (https://policies.google.com/terms) apply.

Twitter
(https://twitter.com/LabsSentinel)

LinkedIn
(https://www.linkedin.com/company/sentinelone)

StackAdapt Pixel