PHOREAL Malware Targets the Southeast Asian Financial Sector

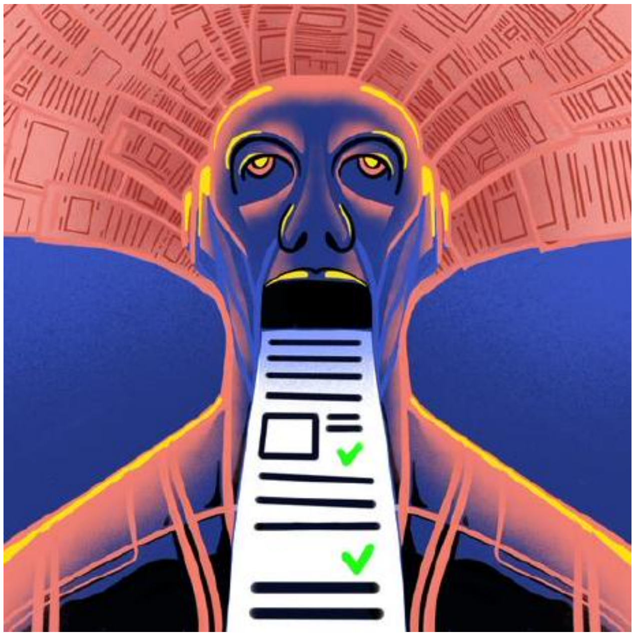
elastic.github.io/security-research/intelligence/2022/03/02.phoreal-targets-southeast-asia-financial-sector/article/

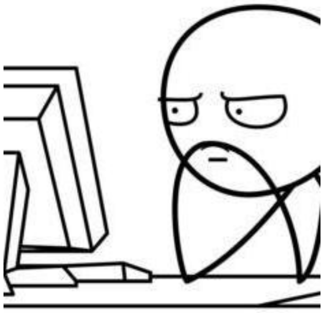
Elastic Security Research

PHOREAL Malware Targets the Southeast

Elastic Security has identified an ongoing campaign targeting a Vietnamese financial services institution with the

PHOREAL RIZZO Malware Backdoor





2022-03-07

Preamble¶

Elastic Security has identified an ongoing campaign targeting a Vietnamese financial services institution with the PHOREAL/RIZZO backdoor. While this malware has been in use for some time, this is the first time that we have observed it loading into memory as a defense evasion and campaign protection technique. Upon analysis of our own observations and previously reported information, we are tracking this activity group (malware + technique + victimology) as REF4322.

What is the threat?¶

PHOREAL/RIZZO is a backdoor allowing initial victim characterization and follow-on post-exploitation operations to compromise the confidentiality of organizations' data. It has been reported in other research as being used exclusively by APT32 (AKA SeaLotus, OceanLotus, APT-C-00, Group G0050).

What is the impact?¶

APT32 largely targets victims with political or economic interests in Southeast Asia, specifically Vietnam.

What is Elastic doing about it?¶

Elastic Security detailed how to triage one of these threat alerts, extracted observables for endpoint and network filtering, and produced a new malware signature for identification and mitigation of the threat across the fleet of deployed Elastic Agents.

Investigation Details¶

While conducting Threat Discovery & Monitoring operations, Elastic Security researchers identified a cluster of `shellcode_thread` Windows memory protection alerts generated from an Elastic Agent endpoint sensor. These particular alerts were interesting because they all occurred within the same cluster, and unusually they targeted the `control.exe` process. The Windows `control.exe` process handles the execution of Control Panel items, which are utilities that allow users to view and adjust computer settings.

Generally when we observe false positives for the `shellcode_thread` protection, it is identified across a broad user-base and in many cases it is attributed to various gaming anti-cheat or DRM (Digital Rights Management) mechanisms. In this case, a single cluster and a Microsoft signed target process was atypical, and worthy of further investigation.

Note

You can read more about Elastic Security's memory protections HERE and about in-memory attacks HERE.

With our interest piqued from the outlier characteristics of the alerts, we investigated further to validate and characterize the threat:

Targeted process is a signed Windows binary
Unsigned loaded .dll

```
...
   "Ext": {
     "mapped_address": 1945501696,
     "mapped_size": 21135360
   },
   "path": "C:\\Windows\\SysWOW64\\tscon32.dll",
   "code_signature": [
     {
       "exists": false
     }
   ],
   "name": "tscon32.dll",
   "hash": {
     "sha1": "007970b7a42852b55379ef4cffa4475865c69d48",
     "sha256": "ec5d5e18804e5d8118c459f5b6f3ca96047d629a50d1a0571dee0ac8d5a4ce33",
     "md5": "2b6da20e4fc1af2c5dd5c6f6191936d1"
   }
 },
...
```

Starting module from the alerting thread

```
...
 "pe": {
   "original_file_name": "CONTROL.EXE"
 },
 "name": "control.exe",
 "pid": 5284,
 "thread": {
   "Ext": {
     "start_address_module": "C:\\Windows\\SysWOW64\\tscon32.dll",
...
```

Alerting memory region metadata

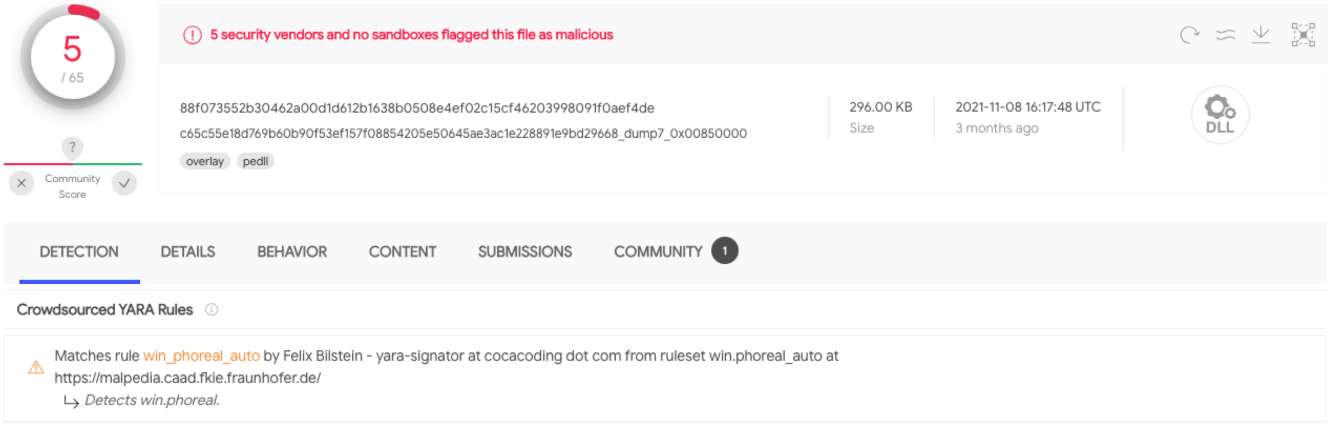
```
...
"memory_region": {`
   "region_size": 73728,
   "region_protection": "RWX",
   "allocation_base": 81395712,
   "bytes_allocation_offset": 0,
   "allocation_type": "PRIVATE",
   "memory_pe_detected": true,
   "region_state": "COMMIT",
   "strings": [
     "QSSSSSSh ",
     ...
     "bad cast",
     "Local\\{5FBC3F53-A76D-4248-969A-31740CBC8AD6}",
     "Netapi32.dll",
     "NetWkstaGetInfo",
     "NetApiBufferFree",
     "\\\\.\\pipe\\{A06F176F-79F1-473E-AF44-9763E3CB34E5}",
     "list<T> too long",
     "{FD5F8447-657A-45C1-894B-D533926C9B66}.dll",
     "DllEntry",
     ...
     ".?AVbad_alloc@std@@",
     "C:\\Windows\\syswow64\\control.exe",
     ":z:zzzzzz7",
     ...
     "InternalName",
     "mobsync.exe",
     "LegalCopyright",
...
```

Thread data for pivoting

```
...
"thread": {
 "Ext": {
   "start_address_bytes": "8bff558bece8e6430000e8db43000050e8bb43000085c0751fff7508e8c94300",
   ...
   "start_address_bytes_disasm": "mov edi, edi\npush ebp\nmov ebp, esp\ncall 0x000043f0\ncall 0x000043ea\npush eax\ncall 
0x000043d0\ntest eax, eax\njnz 0x00000038\npush dword ptr [ebp+0x08]"
 },
...
```

From the example alert we first identify the `start_address_module` which is the dll/module where the thread began. `C:\\Windows\\SysWOW64\\tscon32.dll` is the `start_address_module` for the thread that we've alerted on. It's also the only unsigned dll loaded, so a great place to focus our efforts. When checking the hash value in VirusTotal, to identify previously disclosed information about the sample, we did not see any results.

Digging deeper, we looked at the `start_address_bytes` , which are the first `32` bytes of our alerting thread. We can use the value of the `start_address_bytes` (`8bff558bece8e6430000e8db43000050e8bb43000085c0751fff7508e8c94300`) to search for pivots in VirusTotal by querying `content: {8bff558bec56e83f3e0000e8343e000050e8143e000085c0752a8b750856e821}` . We identified relatively few results, but they included the below entry first submitted in July 2021. \



5 security vendors and no sandboxes flagged this file as malicious

88f073552b30462a00d1d612b1638b0508e4ef02c15cf46203998091f0aef4de
c65c55e18d769b60b90f53ef157f08854205e50645ae3ac1e228891e9bd29668_dump7_0x00850000
overlay pedll

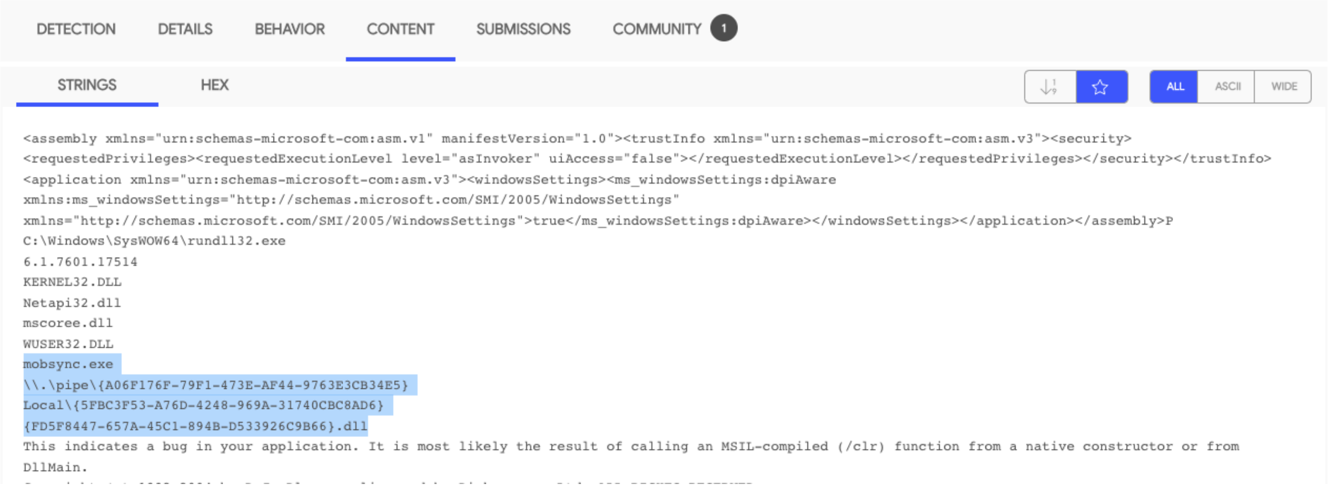
296.00 KB
Size

2021-11-08 16:17:48 UTC
3 months ago

Crowdsourced YARA Rules

Matches rule win_phoreal_auto by Felix Bilstein - yara-signator at cocacoding dot com from ruleset win.phoreal_auto at https://malpedia.caad.fkie.fraunhofer.de/
↳ *Detects win.phoreal.*

VT result matching `start_address_bytes`
In researching the results from VirusTotal, we could see that threat researcher Felix Bilstein (@fxb_b) authored a crowdsourced YARA rule identifying this as the PHOREAL backdoor. Moving on to the `CONTENT` tab, we can compare some of the strings from our alert with what has been previously reported to VirusTotal.



```
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0"><trustInfo xmlns="urn:schemas-microsoft-com:asm.v3"><security>
<requestedPrivileges><requestedExecutionLevel level="asInvoker" uiAccess="false"></requestedExecutionLevel></requestedPrivileges></security></trustInfo>
<application xmlns="urn:schemas-microsoft-com:asm.v3"><windowsSettings><ms_windowsSettings:dpiAware
xmlns:ms_windowsSettings="http://schemas.microsoft.com/SMI/2005/WindowsSettings"
xmlns="http://schemas.microsoft.com/SMI/2005/WindowsSettings">true</ms_windowsSettings:dpiAware></windowsSettings></application></assembly>P
C:\Windows\SysWOW64\rundll32.exe
6.1.7601.17514
KERNEL32.DLL
Netapi32.dll
mscoree.dll
WUSER32.DLL
mobsync.exe
\\.\pipe\{A06F176F-79F1-473E-AF44-9763E3CB34E5}
Local\{5FBC3F53-A76D-4248-969A-31740CBC8AD6}
{FD5F8447-657A-45C1-894B-D533926C9B66}.dll
This indicates a bug in your application. It is most likely the result of calling an MSIL-compiled (/clr) function from a native constructor or from
DllMain.
```

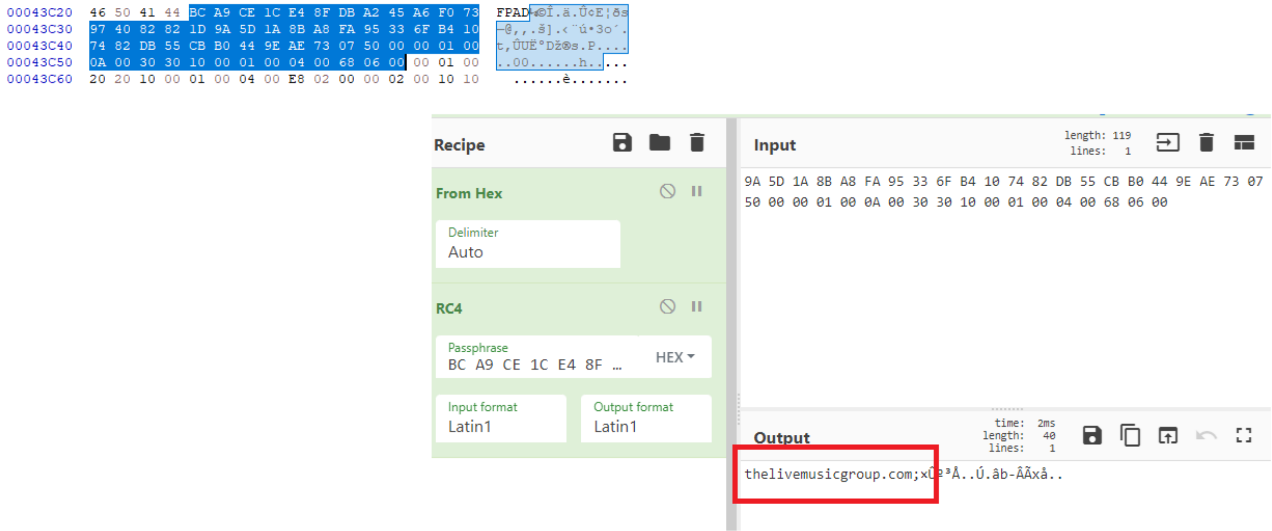
VT result CONTENT tab
Using the unique strings we identified above and the `start_address_bytes` , we can create a YARA signature by converting the unique strings (`$a`) and the `start_address_bytes` (`$b`) into hex values as shown below.

Converted YARA strings

```
strings:
          \\  "\\.\pipe\{A06F176F-79F1-473E-AF44-9763E3CB34E5}"  ascii wide
    $a1 = { 5C 00 5C 00 2E 00 5C 00 70 00 69 00 70 00 65 00 5C 00 7B 00 41 00
            30 00 36 00 46 00 31 00 37 00 36 00 46 00 2D 00 37 00 39 00 46 00
            31 00 2D 00 34 00 37 00 33 00 45 00 2D 00 41 00 46 00 34 00 34 00
            2D 00 39 00 37 00 36 00 33 00 45 00 33 00 43 00 42 00 33 00 34 00
            45 00 35 00 7D 00 }

          \\  "Local\{5FBC3F53-A76D-4248-969A-31740CBC8AD6}"  ascii wide
    $a2 = { 4C 00 6F 00 63 00 61 00 6C 00 5C 00 7B 00 35 00 46 00 42 00 43 00
            33 00 46 00 35 00 33 00 2D 00 41 00 37 00 36 00 44 00 2D 00 34 00
            32 00 34 00 38 00 2D 00 39 00 36 00 39 00 41 00 2D 00 33 00 31 00
            37 00 34 00 30 00 43 00 42 00 43 00 38 00 41 00 44 00 36 00 7D 00 }

          \\  "{FD5F8447-657A-45C1-894B-D533926C9B66}.dll"  ascii
    $a3 = { 7B 46 44 35 46 38 34 34 37 2D 36 35 37 41 2D 34 35 43 31 2D 38 39
            34 42 2D 44 35 33 33 39 32 36 43 39 42 36 36 7D 2E 64 6C 6C }

          \\  PHOREAL start_address_bytes sequence
          \\  mov edi, edi; push ebp; mov ebp, esp; call 0x000043f0;
          \\  call 0x000043ea; push eax; call 0x000043d0; test eax, eax;
          \\  jnz 0x00000038; push dword ptr [ebp+0x08]
    $str_addr = { 8B FF 55 8B EC 56 E8 3F 3E 00 00 E8 34 3E 00 00 50 E8 14 3E
            00 00 85 C0 75 2A 8B 75 08 56 E8 21 }
condition:
    2 of them
```

This rule when deployed to the Elastic Agent will identify PHOREAL to customers and backstop prevention already provided through the `shellcode_thread` memory protection (in customer environments with memory protection turned on). In our case this rule's deployment also enabled the collection of the malicious thread using the same mechanism detailed in our Collecting Cobalt Strike Beacons article.

Shortly after the new YARA artifact was deployed we had a new `malware_signature` alert in hand with the malicious thread captured from memory. Manual binary triage from our Malware Analysis and Reverse Engineering (MARE) Team quickly confirmed the sample was PHOREAL/RIZZO by comparing the structure and functions between our sample and past reporting. Further, they were able to extract an RC4 encrypted domain from an RCDATA resource as described in a 2018 CYLANCE OceanLotus whitepaper.



```
00043C20  46 50 41 44 BC A9 CE 1C E4 8F DB A2 45 A6 F0 73   FPAD¼©Î.ä.Û¢E¦ðs
00043C30  97 40 82 82 1D 9A 5D 1A 8B A8 FA 95 33 6F B4 10   —@‚‚.š].‹¨ú•3o´.
00043C40  74 82 DB 55 CB B0 44 9E AE 73 07 50 00 00 01 00   t‚ÛUË°Dž®s.P....
00043C50  0A 00 30 30 10 00 01 00 04 00 68 06 00 00 01 00   ..00......h.....
00043C60  20 20 10 00 01 00 04 00 E8 02 00 00 02 00 10 10     ......è.......
```

Delimiter: Auto

Passphrase: BC A9 CE 1C E4 8F … HEX

Input format: Latin1

Output format: Latin1

length: 119 lines: 1

```
9A 5D 1A 8B A8 FA 95 33 6F B4 10 74 82 DB 55 CB B0 44 9E AE 73 07
50 00 00 01 00 0A 00 30 30 10 00 01 00 04 00 68 06 00
```

time: 2ms length: 40 lines: 1

```
thelivemusicgroup.com;xÛ²³Å..Ú.âb-ÂÃxå..
```

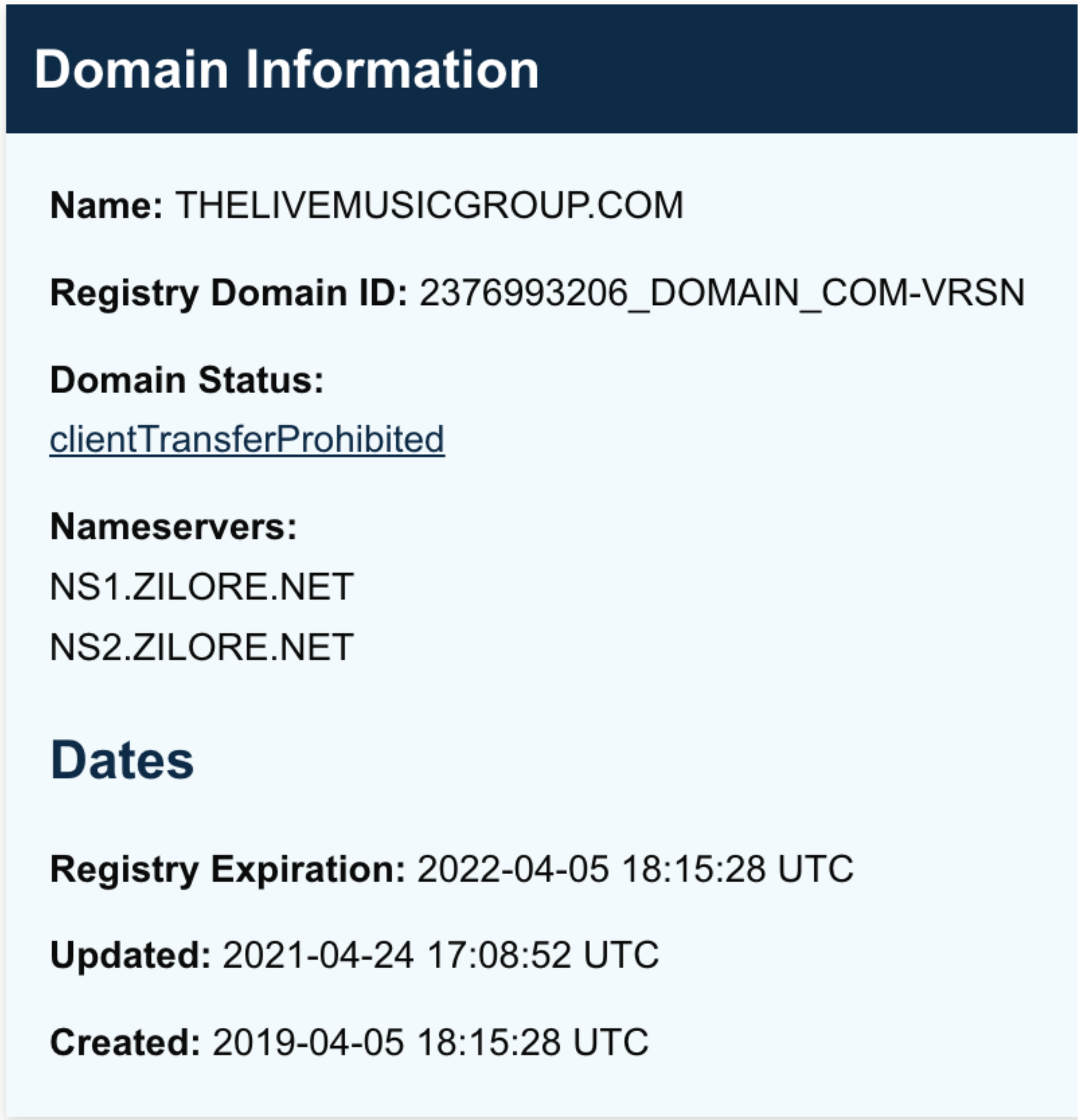
RC4 decrypting binary embedded URL

The domain identified by MARE (`thelivemusicgroup[.]com`) currently resolves to `103.75.117[.]250` which is owned by Oneprovider[.]com, a dedicated server hosting company based out of Canada with data centers distributed globally.

https://ipinfo.io/ query results for 103.75.117[.]250

```
{
  "ip": "103.75.117[.]250",
  "city": "Hong Kong",
  "region": "Central and Western",
  "country": "HK",
  "loc": "22.2783,114.1747",
  "org": "AS133752 Leaseweb Asia Pacific pte. ltd.",
  "timezone": "Asia/Hong_Kong",
  "asn": {
    "asn": "AS133752",
    "name": "Leaseweb Asia Pacific pte. ltd.",
    "domain": "leaseweb.com",
    "route": "103.75.117[.]0/24",
    "type": "hosting"
  },
  "company": {
    "name": "Oneprovider.com - Hong Kong Infrastructure",
    "domain": "oneprovider[.]com",
    "type": "hosting"
  },
  "privacy": {
    "vpn": false,
    "proxy": false,
    "tor": false,
    "relay": false,
    "hosting": true,
    "service": ""
  },
  "abuse": {
    "address": "1500 Ste-Rose LAVAL H7R 1S4 Laval Quebec, Canada",
    "country": "CA",
    "email": "info@oneprovider.com",
    "name": "ONE PROVIDER",
    "network": "103.75.117[.]0/24",
    "phone": "+1 514 286-0253"
  },
  "domains": {
    "ip": "103.75.117[.]250",
    "total": 2,
    "domains": [
      "thelivemusicgroup[.]com",
      "cdn-api-cn-1[.]com"
    ]
  }
```

Most of the interesting information about the domain is privacy guarded, but the “Updated” and “Created” dates in the below figure might be useful for bounding how long this domain has been used maliciously.



Domain Information

Name: THELIVEMUSICGROUP.COM

Registry Domain ID: 2376993206_DOMAIN_COM-VRSN

Domain Status:
clientTransferProhibited

Nameservers:
NS1.ZILORE.NET
NS2.ZILORE.NET

Dates

Registry Expiration: 2022-04-05 18:15:28 UTC

Updated: 2021-04-24 17:08:52 UTC

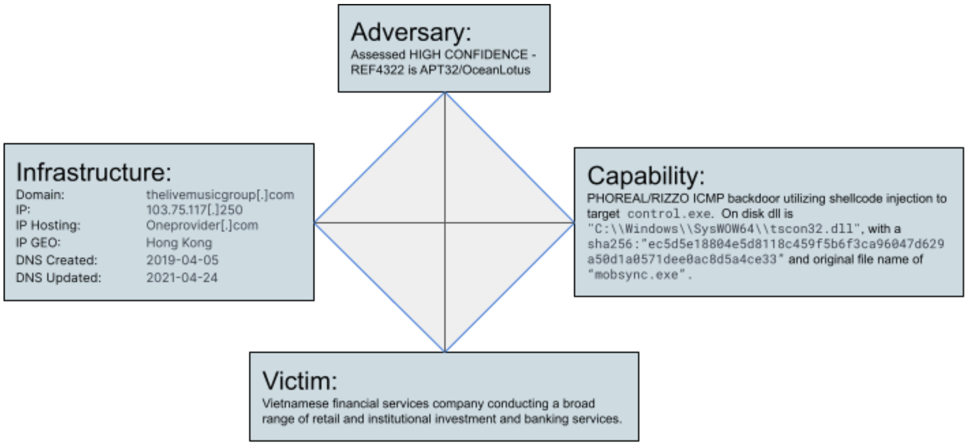
Created: 2019-04-05 18:15:28 UTC

https://lookup.icann.org/lookup for `thelivemusicgroup[.]com`

The Elastic Agent appears to have been deployed post-compromise which limited our ability to determine the vector of initial access. A 2017 Mandiant report indicates that PHOREAL may be deployed in an “establish foothold” capacity to allow for victim triage and follow-on post-exploitation tools.

Analysis¶

Elastic Security utilizes the Diamond Model to describe high-level relationships between the adversaries and victims of intrusions.



Adversary:
Assessed HIGH CONFIDENCE - REF4322 is APT32/OceanLotus

Infrastructure:

Domain:	thelivemusicgroup[.]com
IP:	103.75.117[.]250
IP Hosting:	Oneprovider[.]com
IP GEO:	Hong Kong
DNS Created:	2019-04-05
DNS Updated:	2021-04-24

Capability:
PHOREAL/RIZZO ICMP backdoor utilizing shellcode injection to target `control.exe`. On disk dll is `"C:\\Windows\\SysWOW64\\tscon32.dll"`, with a `sha256:"ec5d5e18804e5d8118c459f5b6f3ca96047d629a50d1a0571dee0ac8d5a4ce33"` and original file name of `"mobsync.exe"`.

Victim:
Vietnamese financial services company conducting a broad range of retail and institutional investment and banking services.

REF4322 Diamond Model Analysis

Adversary Assessment Justification¶

We assess with high confidence based on observed activity and previous reporting that REF4322 is APT32/OceanLotus and the actor behind this incident. APT32 has been active since 2014 notably targeting Southeast Asian governments and businesses or other international businesses with interests in Vietnam. APT32 is the only group currently identified as operating the PHOREAL backdoor, and our victim matches the geographic and industry vertical profile of typical and specific prior APT32 victims.

Conclusion¶

YARA Rules¶

We have created a YARA rule to identify this PHOREAL activity.

Defensive Recommendations¶

The following steps can be leveraged to improve a network's protective posture:

1. Enable Elastic Security Memory Protection on Windows endpoints
2. Leverage the included YARA signatures above to determine if PHOREAL activity exists within your organization
3. Monitor or block network traffic to or from identified network IOCs and remediate impacted systems accordingly.

References¶

The following research was referenced throughout the document:

Observables¶

Indicator	Type	Reference	Notes
`thelivemusicgroup[.]com`	domain-name		C2 domain encrypted in malware
`103.75.117[.]250`	ipv4-addr		Resolved IP of `thelivemusicgroup[.]com`
`ec5d5e18804e5d8118c459f5b6f3ca96047d629a50d1a0571dee0ac8d5a4ce33`	SHA256	`tscon32.dll`	PHOREAL dll

Artifacts¶

Artifacts are also available for download in both ECS and STIX format in a combined zip bundle.

Download indicators.zip

Last update: March 8, 2022
Created: March 7, 2022