Go to listing page

APT40: A State-Sponsored Cyber Espionage Group Targeting North America And Europe to Obtain Advanced Naval Technology

Threat Actor

Threat Actor Profile

Origin: 2013

Aliases: Leviathan, TEMP.Jumper, TEMP.Periscope, APT 40

Key Target Sectors: Transportation, Government / Military, Educational, InformationTechnology, Communication, Manufacturing, Enterprise Services

Attack Vectors: Spam Email, Spear phishing, Phishing, and Luring.

Target Region: Western Europe, North America, South-East Asia

Malware Used: ScanBox, WindTone, Grillmark, BlackCoffee, Gh0st, China Chopper, WilDelk, FreshAir, KorPlug, HomeFry, RedMage, FieldGoal, RedMage, AirBreak, Js Spy, Murkytop, Beacon, Murkyshell, Orz, LunchMoney, and NanHaiShu.

Tools Used: PaperRush, Photo

Vulnerabilities Exploited: CVE-2017-0199, CVE-2012-0158, CVE-2017-11882, and CVE-2017-8759

Overview

APT40 is a cyberespionage threat group linked to the Chinese government, known for targeting critical technologies and traditional intelligence firms in North America, Europe, and East Asia. The group is conducting cyber operations since at least

2013, and its espionage activities mostly support China’s naval modernization attempt. This cyberespionage group was previously reported as TEMP.Periscope and TEMP.Jumper. Most recently, in early-2019, it was again seen attempting to steal secrets related to advanced technology to support the development of Chinese naval capabilities.

Which organizations has the group targeted?

Since 2013, the cyberespionage group has been targeting engineering, transportation, and defense sectors, along with a specific interest in maritime technologies. In Dec. 2016, China’s People Liberation Army Navy (PLAN) seized a U.S. Navy’s Unmanned Underwater Vehicle (UUV) serving in the South China Sea. The cyber event paralleled China’s actions in cyberspace. Within a year, the group was observed disguising as a UUV manufacturer and was observed targeting universities engaged in marine research. More recently in early 2019, specific targeting of countries strategically crucial to the Belt and Road Initiative has been observed. The group also targets China’s neighbourhood countries for traditional intelligence, particularly organizations that are having operations in Southeast Asia or associated in South China Sea disputes.

What is their motivation behind the attacks?

The group is focused on targeting countries critical to China’s Belt and Road Initiative (i.e., Cambodia, Belgium, Germany, Hong Kong, Philippines, Malaysia, Norway, Saudi Arabia, Switzerland, the United States, and the United Kingdom). The cyberespionage group also targeted universities and research centers involved in marine research, mostly from the USA. This was done with the intent to access advanced technology to accelerate the growth of the Chinese maritime industry. These attacks on the naval research firms ultimately support China’s dream to establish a blue-water navy in South-China sea.

Modus Operandi

This group has been observed using multiple methods for initial compromise, including web server exploitation, strategic web compromises, phishing campaigns delivering backdoors, both publicly available as well as custom made. The group mostly relies on web shells for an initial foothold inside the targeted organization. A web shell can give regular access to victim’s environments, enable lateral movement, and re-infect victim systems if required. The spear

Share Blog Post

phishing emails usually use malicious attachments, although malicious Google Drive links have also been observed. In these phishing campaigns, the group has been observed using vulnerabilities like CVE-2012-0158, CVE-2017-0199, CVE-2017-8759, and CVE-2017-11882, within days of their disclosure.

For APT40, successful completion of an operation usually means transferring and gathering information out of the target network, which may include moving files via many systems before reaching the destination. It consists of the process where consolidated files are obtained from victim networks, and the data is compressed and encrypted using an archival tool rar.exe before exfiltration. The group also developed a tool named as "PaperRush" to improve the efficiency of their data theft and targeting tasks.

Known tools and malware

The group is known to be using various first-stage backdoors, custom malware, publicly available reconnaissance tools to carry out their cyber operations. Such tools include ScanBox, WindTone, Grillmark, BlackCoffee, Gh0st, WilDelk, KorPlug, HomeFry, RedMage, FieldGoal, RedMage, Eviltech, and Js Spy. This group also uses genuine software within the victim environment (RDP, SSH), publicly available tools (MurkyShell, MurkyTop), an array of native Windows capabilities, as well as custom scripts to accomplish internal reconnaissance. For lateral movement, the group uses native Windows utilities such as net.exe (a network resources management tool) and at.exe (a task scheduler). For initial foothold, the group also use first-stage backdoors such as AirBreak, FreshAir, Photo, BadFlick, China Chopper, and Beacon, and targets VPN and remote desktop credentials. At later stages, for privilege escalation and password hash dumping, the group uses custom and publicly available credential harvesting tools like HomeFry, Windows Credential Editor (WCE), and Windows Sysinternals ProcDump.

Malicious programs used by APT40

- **BlackCoffee** - A backdoor that targets the Windows platform-based systems.
- **Gh0st** - A Trojan horse developed to target Windows-based system.
- **Orz** - A Trojan that comes hidden in malicious programs.
- **NanHaiShu** - A remote access tool and JScript backdoor used by APT40.
- **China Chopper** - A 4KB Web-shell used by Chinese and other malicious threat actors.
- **KorPlug** - A Trojan horse that opens a back door and may steal details from

the compromised computer.

- **HomeFry** - A 64-bit Windows password dumper/cracker that has previously been used in conjunction with AirBreak and BadFlick backdoors.
- **FreshAir** - A malicious program used by APT40 for an initial foothold in the targeted organization.
- **RedMage**, **FieldGoal**, and **Grillmark** - Backdoors used by APT40 for an initial foothold in a targeted organization.
- **BadFlick** - A backdoor that can modify the file system, generate a reverse shell, and its command and control (C2) configuration.
- **LunchMoney** - An uploader that can exfiltrate files to Dropbox.
- **AirBreak** - A JavaScript-based backdoor, that retrieves commands from hidden strings in compromised web pages.
- **Js Spy** - A JavaScript-based backdoor used to get an initial foothold in the targeted organization.
- **Murkyshell** - A custom malware, known to be used by APT40.

Known Commercial/Open Source Tools used by APT40

- **Beacon** - A backdoor that is commercially available as part of the Cobalt Strike software platform.
- **Murkytop** - A command-line

reconnaissance tool to execute files as a different user.

- **ScanBox** - This Javascript file is a framework used for reconnaissance purpose.
- **WindTone** and **WilDelk**- Command-line reconnaissance tools known to be used by APT40.

Custom tools used by APT40

- **PaperRush** - It is used to improve the efficiency of data theft and targeting activities.
- **Photo** - A DLL backdoor, also known publicly as Derusbi
- **Eviltech** - A JavaScript pattern, that implements a RAT with assist for importing, downloading, and working arbitrary JavaScript.

Known zero-day vulnerabilities exploited by APT40

- **MSCOMCTL.OCX RCE Vulnerability (CVE-2012-0158)** - A remote code-execution vulnerability in the Microsoft Office.
- **WordPad Remote Code Execution Vulnerability (CVE-2017-0199)** - A remote code-execution vulnerability in Microsoft Office/Wordpad.
- **.NET Framework Remote Code**

Execution Vulnerability (CVE-2017-8759) - A remote code-execution vulnerability that allows an attacker to execute code remotely via a malicious document/application.

- **Microsoft Office Memory Corruption Vulnerability (CVE-2017-11882)** - A memory-corruption vulnerability in the Microsoft Office.

Attribution

The group’s targeted victims are linked to Chinese state interests, and various technical artifacts are supporting the fact that this actor is based in China. Also, the operational times of this group’s activities indicate that it is probably centered around China Standard Time (UTC +8). Many command and control (C2) domains linked with this group were initially registered by China-based domain resellers and had Whois records with Chinese location information, implying a China-based infrastructure procurement process. The group also used several Internet Protocol (IP) addresses placed in China to manage its operations. In one case, a log file recovered from an open indexed server exposed an IP address (112.66.188[.]28) located at Hainan, China. It was used to control the command and control node that was interacting with malware on victim machines. All of the logins to this C2 node were configured with Chinese language settings.

Prevention

APT40 uses its custom tools and sophisticated malware, and to prevent such advanced threats, traditional anti-malware solutions may not be sufficient. It is recommended to implement an in-depth security model that assures URL filtering, behavior-based detection methods, and sandboxing. Using smart usage monitoring tools leveraging orchestration technology to detect any unusual behavior, prevent it, and contain it from impacting critical systems of organizations. Sharing of Strategic and Tactical Threat Intelligence with trusted partners, ISACs and regulatory bodies can also help organizations develop and practice shared strategies for combating such threats. To detect and prevent the sophisticated tactics of lateral movement, an enterprise-level security solution is a must to monitor both endpoint behavior and network traffic. It should be able to detect any signs of lateral movements inside the network and flag them for review by a security analyst.

Since the main focus of APT40 is to steal intellectual property, deploying data loss prevention (DLP) systems to monitor data-atrest, data-in-motion, and data-at-end-points can help. Also, the implementation of advanced detection techniques to find malware, e.g., sandbox execution for analyzing malware can help prevent attacks from such threats. APT40 is also known to use spear phishing, which could be prevented by inculcating situational awareness among all employees along with phishing simulations, strict policies, and periodic refreshers that discourage unsafe behaviors. Given the prevalence of attacks used by APT40 that exploit known vulnerabilities, rigorous patch management, and vulnerability assessments practices are a must.

Indicators of Compromise

MD5
00f952c54f1189bf9583d9fb066be54a
055bc765a78da9cc759d1ba7ac7ac05e
0cb26112cb09d268ccbfe10ac59765df
0dfed59e581c181baeabb5d936c902ce
10c6029fbc0a2770b9686cf31d58067a
166694d13ac463ea1c2bed64fbbb7207
17dbbda8cd63c255d647ab7c423367e5
1c35a87f61953baace605fff1a2d0921
1c6ef040cd7121915245677eef5a3180
2366918da9a484735ec3a9808296aab8
25fc656f3756c7d58aa15aa7e9fae2dc
2754975fb01c931f070d880b224eaee7
2a38ff33240e20caabfc53524a840dfd

2bf998d954a88b12dbec1ee96b072cb9

302003a7ee0d848c98df4bb2b7c720cd

35b82e945de3c49d52283f2caea979f5

36db1bad238251aee8a7aed3d6611ee0

388ba6c81f1a1a9272501e75cf4f0004

3cc6ac12134842539b5e09666953d636

3d1488a737aa2dbfbfe27bb4f471dbb5

3de2a22babb69e480db11c3c15197586

3e169f4fafaf7183d969c89509eb5323

3eb6f85ac046a96204096ab65bbd3e7e

3fefa55daeb167931975c22df3eca20a

40528e368d323db0ac5c3f5e1efe4889

494de66128649e8a0402f832f59e2461

4b18b1b56b468c7c782700dd02d621f4

4bfe05f182aa273e113db6ed7dae4bb8

4ca03bc4fe19c40726fdf2522fdf99e2

4e143cd287cd32901959db9a2a1caf6c

4fc312db8fe933dac24f6d442154f4d0

51da8bd4728d910304c87d992a54cd8a

51e21a697aec4cc01e57264b8bfaf978

52d55e7c2fe820278c7e65e67bce06dd

552c0ee63dbab148688d2cc8644b41f0

593bc6a2e29ec3dde3571c3b8422a11c

5e6e4581613bb5938f3b7eb84724aa2a

5ef4eff48da3d64d5bf598f3279e463b

6051a9adad0df05f858ef18bd567d182

62fb42f4697c206f1338cee8b0ea00c7

65225397c292e5a0e049776ed352158c

681b98d0135ff6358b1cf019825a2919

6d250a11f68b1fd4ed0505fb2965b6f7

6e843ef4856336fe3ef4ed27a4c792b1

6f4d0bdc31f082f770eae395216eef08

71aeeaba2f5cfd80fb98a2df06bdad23

72a7fd2b3d1b829a9f01db312fdd1cd7

758d572af84e6a098b995191fa713cf3

7691ae0369ba3b17198c98ba7059c26a

7d34caa19b129f44b48b9497a4970e2a

7dedb394533f86fe97eddaf0a193baf4

7ed9b4031473ebbe8694d4d712ff46f5

824c92e4b27026c113d766c0816428a0

85862c262c087dd4470bb3b055ef8ea5

955af7983ab57c1e2f760405fe56e607

97326e72e700ba4912459b64ded9cdcf

99d8ea34d18432588622ae564114971d

9a643c7f7483c5a30815431943075522

9c1bd3fdd7541c770da2824f1fcf3b1c

9e035ad76bfe8bde87e5ee362af5dc63

a23d7b6a81dc0b460294e8be829f564d

a29f3abada0199ddd6cde01ba50a3063

a545a710b0acf3a4c83d3b9e57f22515

a91c9a2b1bc4020514c6c49c5ff84298

a9ad68065f85b28c87cf6df1657dff81

a9e7539c1ebe857bae6efceefaa9dd16

aa4d99ec6913b048d60ddcd1f17e3dba

Aa8c545a312597c7469f6555cad2dbbb

ab2756872719b7f7878a1bc4b062b056

ab37ed19d7300e673e66dbd4fec990b1

ac073ad83555f3748d481bcf796e1993

Adc669c40dc71b8d1138e16d9343baae

b5678e77398b2bae81b15c603b70fb14

b7499525634a4099d2e19b330e0910d1

b7e7186d962d562af6a5d10a25d19b02

B86b6cc96d587a65afb266eedec0b695

baf296853822e8d984e1fee586bb4927

Bd9e4c82bf12c4e7a58221fc52fed705

bf6d3f52ab8176122be858ddccc22148

C0b31a090a263d67de958e7ccb68ebe3
c0e85b34697c8561452a149a0b123435
C1c5634c515303440062d962ce3e4960
c52464e9df8b3d08fc612a0f11fe53b2
C8594dbe90041eb901c7a0aae280415e
D1d254d1460e1e3c5339f20c78c78173
d2fb01629fa2a994fbd1b18e475c9f23
d452c1a73a281b772386f0ca70b1ac5e
Da5596183958529c95626a6c9dc875a1
Db72397c05e31456718c732514531df5
ddbd64b7f6588a47d242c8f12d62af96
Df9f8cc805dc67c16227f46f573da6d7
e1123a77b36c8dde7bd2e778fba6ecda
e4944351000afc07ccecd9929251d744
E72583654007eaadc90eb7dc4a7baecc
E82622e08bb27b63ea82de8017b18079
E890fa6fd8a98fec7812d60f65bf1762
ee8d2f20877f77f39814454d40a4e295
f74ccb013edd82b25fd1726b17b670e5
Fa7f84fad695c1aa93458071e0b27f6e
fd402446609261a8071ef298c9d1d660
fe07da37643ed789c48f85d636abcf66

SHA256
cdf6e2e928a89cbb857e688055a25e37a8d8b
8b90530bd52c8548fb544f66f1f
c7fa6f27ec4f4142ae591f2dd7c63d04643194
5f03c87dbed88d79f55180a46d
39c952c7e14b6be5a9cb1be3f05eafa22e111
5806e927f4e2dc85d609bc0eb36
146aa9a0ec013aa5bdba9ea9d29f59d48d43
bc17c6a20b74bb8c521dbb5bc6f4

IP Addresses

185.106.120[.]206
193.180.255[.]2
68.65.123[.]230
82.118.242[.]242
82.118.242[.]243

Domains

scsnewstoday[.]com
thyssenkrupp-marinesystems[.]org

TAGS

tempperiscope paperrush apt40 leviathan

Posted on: July 26, 2019

← PREVIOUS
Honing the Art of Cyber Intelligence

→ NEXT
Building Cyber Fusion Center the Ri...

Recent Posts

April 02, 2024

Navigating the AI Terrain: 10 Key Questions to Ask Cybersecu...

When researching cybersecurity vendors, it's nearly impossible to avoid being ...

cybersecurity solutions

artificial intelligence ai

March 26, 2024

Building Resilient Supply Chains with Shared Intelligence

Pose the question to any CISO, and they'll confirm: protecting the integrity o...

supplier information sharing networks

supply chain security

+ 2 more

February 16, 2024

Generative AI and Cybersecurity Operations: The Criticality ...

As cyber threats grow more sophisticated and diverse, security operations cent...

security operations

cybersecurity standards

+ 2 more

More from Cyware

Stay updated on the security threat landscape and technology innovations at Cyware with our threat intelligence briefings and blogs.

Daily Threat Briefing

Cyware Daily Threat Intelligence, April 02, 2024

Weekly Threat Briefing

Cyware Weekly Threat Intelligence, March 25–March 29, 2024

Monthly Threat Briefing

Cyware Monthly Threat Intelligence, February 2023

The Virtual Cyber Fusion Suite

Collaborate

Intel Exchange

Orchestrate

Respond

Explore Solutions

Capabilities

Resource Library

Use Cases

Products

Cyber Fusion Center

Threat Intelligence Platforms (TIP)

Intel Exchange

Intel Exchange Lite

Collaborate

Security Orchestration and Automation (SOAR)

Respond

Orchestrate

Partners

Channel Partners

MSSPs

Technology Alliances

Open APIs

MISP

Register a Deal

CywareOne Login

Resources

Resource Library

Cyware Labs: Research & Threat Briefings

Security Guides

Free Threat Intel Feeds

Webinars & Videos

Community Resources

Cyware Academy

Company

Leadership

Careers **We're Hiring**

Cyware in the News

Press Releases

Compliance

Contact Us

Learn More

Blog

TIP Replacement

SOAR Replacement

Request a Demo

Support

Legal

Threat Intelligence Ecosystem

Solutions for ISACs, ISAOs, and CERTs

Solutions for ISAC, ISAO, and CERT Members

Intel Exchange Spoke

Cyware Browser Extension

Get in touch with us now! 1-855-692-9927

Terms of Use Pri .cy

1

023