Recorded Future

CYBER THREAT ANALYSIS

Chinese Threat Actor TEMP.Periscope Targets UK-Based Engineering Company Using Russian APT Techniques

By Insikt Group
Recorded Future

CTA-2018-1113

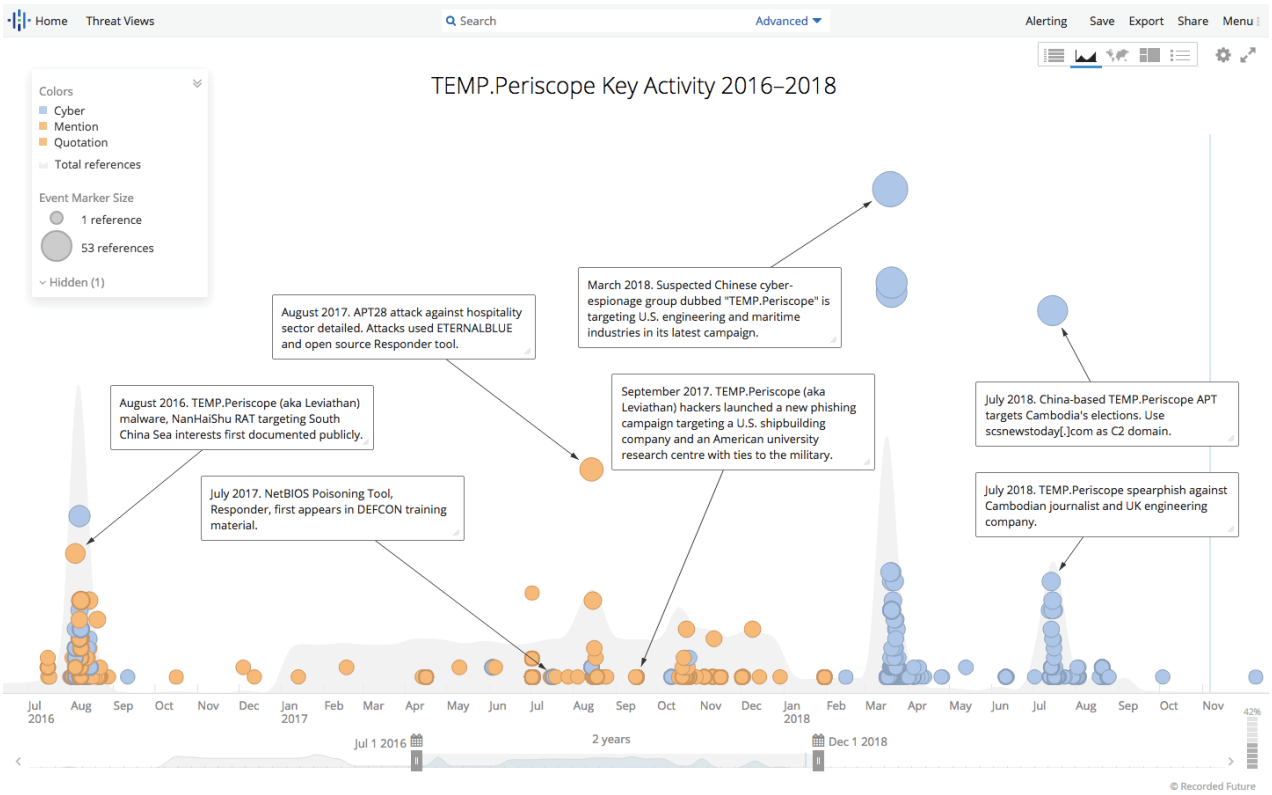
Scope Note: Recorded Future's Insikt Group analyzed network indicators of compromise and TTPs relating to an intrusion incident targeting a U.K.-based engineering company. Sources include Recorded Future's product, VirusTotal, ReversingLabs, DomainTools Iris, and PassiveTotal, along with third-party metadata and common OSINT techniques.

This report will be of greatest interest to organizations within the high-tech engineering industries in the U.S., Europe, and Japan, as well as those investigating Chinese state-sponsored cyberespionage.

Executive Summary

Employees of a U.K.-based engineering company were among the targeted victims of a spearphishing campaign in early July 2018. The campaign also targeted an email address possibly belonging to a freelance journalist based in Cambodia who covers Cambodian politics, human rights, and Chinese development. We believe both attacks used the same infrastructure as a reported campaign by Chinese threat actor TEMP.Periscope (also known as Leviathan), which targeted Cambodian entities in the run-up to their July 2018 elections. Crucially, TEMP.Periscope's interest in the U.K. engineering company they targeted dates back to attempted intrusions in May 2017.

Based on the available data and evidence outlined in this report, Recorded Future assesses with medium confidence that Chinese threat actor TEMP.Periscope reused publicly reported, sophisticated TTPs from Russian threat groups Dragonfly and APT28 to target the U.K. engineering company, likely to gain access to sensitive and proprietary technologies and data. We believe TEMP.Periscope reused published TTPs either to increase the group's chances of success in gaining access to the victim network or to evade attribution by laying false flags to confuse researchers.



Timeline of selected APT28, Dragonfly, and TEMP.Periscope TTP disclosures and activity.

Key Judgments

- Attackers likely used a command and control (C2) domain, scsnewstoday[.]com, that was identified in a recent TEMP.Periscope campaign targeting the Cambodian government.
- The attackers used a Chinese email client, Foxmail, to send the spearphishing attack.
- A unique technique documented as a Dragonfly TTP in targeting critical infrastructure was used in the attack. The technique attempts to acquire SMB credentials using a “file://” path in the spearphish calling out to a malicious C2.
- The attack probably made use of a version of the open source tool Responder as an NBT-NS poisoner. APT28 used Responder in attacks against travelers staying at hotels in 2017.
- The U.K. engineering company was previously targeted by TEMP.Periscope in a May 2017 campaign with the same C2 infrastructure that was used in targeting U.S. engineering and academic entities later in September 2017, as detailed in Proofpoint’s Leviathan report.

Background

TEMP.Periscope is a state-sponsored Chinese threat actor that first came to public prominence in October 2017, when reports surfaced about a group called Leviathan. Leviathan used a combination of unique and open source tooling to target the maritime and defense industries for espionage purposes. The report detailed coverage of the group dating back to at least 2014.

Reporting emerged months later highlighting further activity against the maritime and defense sectors that mainly targeted companies in the U.S. and Europe and included more details on the group's TTPs. The activity was tagged with a new threat actor name, TEMP.Periscope, but the report authors noted that Leviathan and TEMP.Periscope were the same group.

The increased targeting of high-tech marine engineering entities coincided with the growing regional tensions surrounding China's claims for much of the South China Sea (SCS) territory. Chinese cyberespionage targeting countries neighboring the South China Sea continued to escalate in 2018, with reports of TEMP.Periscope targeting Cambodia ahead of their July 2018 elections. Additionally, attacks such as the one uncovered against a U.S. Navy contractor in early 2018, resulting in the theft of a massive amount of highly sensitive data that included plans to develop a submarine-based, supersonic anti-ship missile, demonstrate China's continued targeting of cutting-edge naval technology to bridge the technological gap with the U.S.

Threat Analysis

The Infection Vector

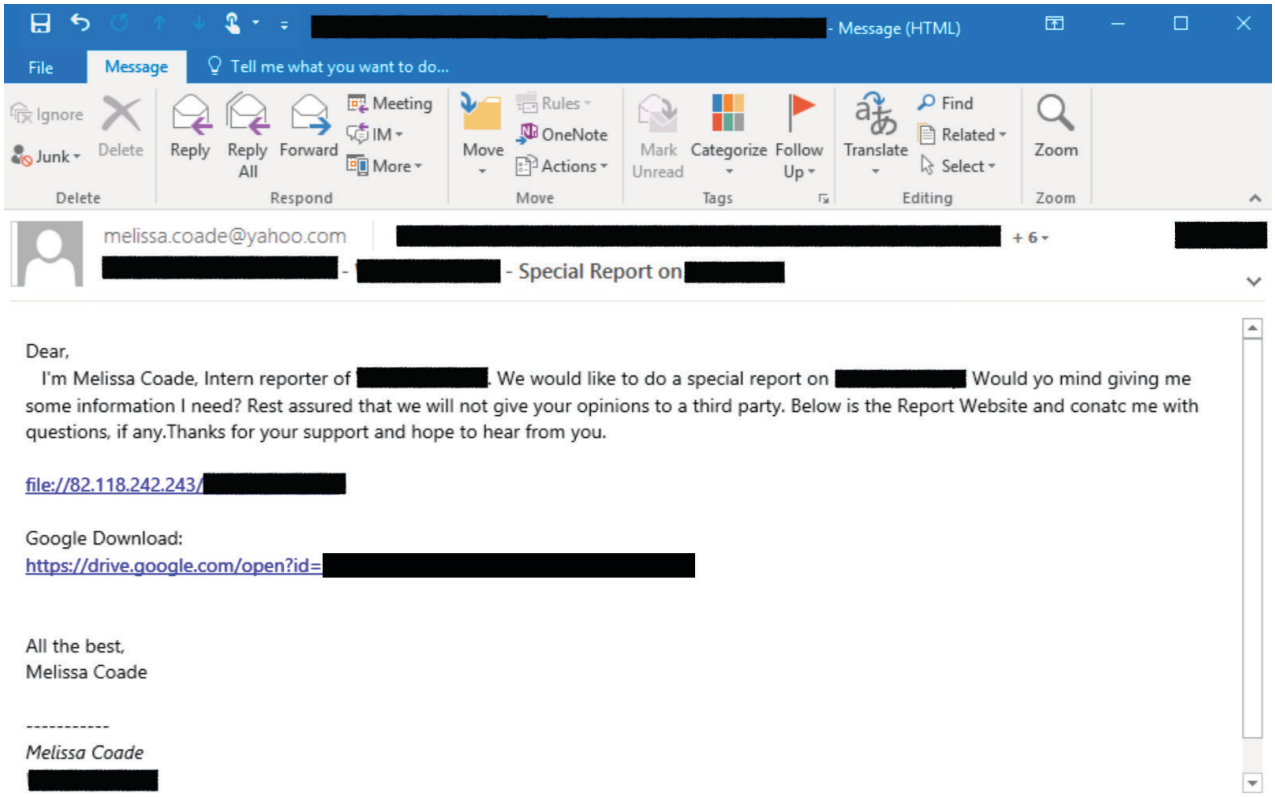
The attempted intrusion we studied targeted the network of a U.K. company that provides specialist engineering solutions. The U.K. engineering company shared details of the attempted spearphish with Recorded Future, and the following IOCs served as a starting point for our investigation.

Indicator	Description
193.180.255[.]2	Spearphish sent from this IP
82.118.242[.]243	Source of SMB credential stealing attempts
WIN-AB2I27TG6FK	NetBios server name of the device sending the spearphish
WIN-PRH492RQAFV	NetBios server name of the device conducting SMB credential stealing

Email headers revealed that the spearphish was sent on July 6, 2018 at 9:30 AM UTC, via Foxmail. Foxmail is a freeware email client developed by Tencent, one of the three largest internet services companies in China. Foxmail boasts over three million daily users in China and has previously been associated with Chinese APT activity.

In addition to email addresses belonging to the U.K. engineering company's employees, the same spearphish was also sent to an email address possibly belonging to a journalist based in Cambodia. The sender account was spoofing an Australian journalist and lawyer, who among other things writes about Cambodian civil and social matters and has written for the Phnom Penh Post.

In a spearphishing campaign targeting the Cambodian elections in July 2018, Chinese threat actor TEMP.Periscope spoofed the sender address and impersonated a worker from a Cambodian nongovernmental organization (NGO).



Snippet of a spearphish email shared by the targeted U.K. engineering company.

The email contained two malicious links. The first, a "file://" link, if clicked, would generate an SMB session. The second link was to a .url file that was also configured to create an outbound SMB connection.

The threat actor masqueraded as a Cambodian reporter requesting further information from the victim to be uploaded to her "report website." However, spelling and punctuation errors in the message alerted network defenders at the victim organization.

Our analysis of the metadata contained within the email header and a subsequent controlled interaction with the file share over SMB revealed several interesting characteristics of the attempted intrusion.

Responder: The "NetBIOS Poisoner"

First, we analyzed the SMB file path link. We observed the hostname WIN-PRH492RQAFV on C2 82.118.242[.]243 when it attempted to acquire SMB credentials from the victim network. We then noted the hostname WIN-PRH492RQAFV was hardcoded within several forked versions of a Python hacktool called Responder on GitHub. One version of Responder with this hostname was found in a build of P4wnP1[1] that was uploaded to BeeBin, a free file upload service, and another version with the same hostname was found within PiBunny.

[1] P4wnP1 is a highly customizable USB attack platform based on a Raspberry Pi Zero computer.

```
1511                ("Tag2ASNId",             "\xA2"),
1512                ("Tag2ASNIdLenOfLen",     "\x81"),
1513                ("Tag2ASNIdLen",          "\xE9"),
1514                ("Tag3ASNId",             "\x04"),
1515                ("Tag3ASNIdLenOfLen",     "\x81"),
1516                ("Tag3ASNIdLen",          "\xE6"),
1517                ("NTLMSSPSignature",      "NTLMSSP"),
1518                ("NTLMSSPSignatureNull",  "\x00"),
1519                ("NTLMSSPMessageType",    "\x02\x00\x00\x00"),
1520                ("NTLMSSPNtWorkstationLen","\x1e\x00"),
1521                ("NTLMSSPNtWorkstationMaxLen","\x1e\x00"),
1522                ("NTLMSSPNtWorkstationBuffOffset","\x38\x00\x00\x00"),
1523                ("NTLMSSPNtNegotiateFlags","\x15\x82\x89\xe2"),
1524                ("NTLMSSPNtServerChallenge","\x81\x22\x33\x34\x55\x46\xe7\x88"),
1525                ("NTLMSSPNtReserved","\x00\x00\x00\x00\x00\x00\x00\x00"),
1526                ("NTLMSSPNtTargetInfoLen","\x94\x00"),
1527                ("NTLMSSPNtTargetInfoMaxLen","\x94\x00"),
1528                ("NTLMSSPNtTargetInfoBuffOffset","\x56\x00\x00\x00"),
1529                ("NegTokenInitSeqMechMessageVersionHigh","\x06"),
1530                ("NegTokenInitSeqMechMessageVersionLow","\x03"),
1531                ("NegTokenInitSeqMechMessageVersionBuilt","\x80\x25"),
1532                ("NegTokenInitSeqMechMessageVersionReserved","\x00\x00\x00"),
1533                ("NegTokenInitSeqMechMessageVersionNTLMType","\x0f"),
1534                ("NTLMSSPNtWorkstationName
1535                ("NTLMSSPNTLMChallengeAVPa
1536                ("NTLMSSPNTLMChallengeAVPairsLen","\x0a\x00"),
1537                ("NTLMSSPNTLMChallengeAVPairsUnicodeStr","SMB3"),
1538                ("NTLMSSPNTLMChallengeAVPairs1Id","\x01\x00"),
1539                ("NTLMSSPNTLMChallengeAVPairs1Len","\x1e\x00"),
1540                ("NTLMSSPNTLMChallengeAVPairs1UnicodeStr","WIN-PRH492RQAFV"),
1541                ("NTLMSSPNTLMChallengeAVPairs2Id","\x04\x00"),
1542                ("NTLMSSPNTLMChallengeAVPairs2Len","\x1e\x00"),
1543                ("NTLMSSPNTLMChallengeAVPairs2UnicodeStr","SMB3.local"),
1544                ("NTLMSSPNTLMChallengeAVPairs3Id","\x03\x00"),
1545                ("NTLMSSPNTLMChallengeAVPairs3Len","\x1e\x00"),
1546                ("NTLMSSPNTLMChallengeAVPairs3UnicodeStr","WIN-PRH492RQAFV.SMB3.local"),
1547                ("NTLMSSPNTLMChallengeAVPairs5Id","\x05\x00"),
1548                ("NTLMSSPNTLMChallengeAVPairs5Len","\x04\x00"),
1549                ("NTLMSSPNTLMChallengeAVPairs5UnicodeStr","SMB3.local"),
1550                ("NTLMSSPNTLMChallengeAVPairs7Id","\x07\x00"),
1551                ("NTLMSSPNTLMChallengeAVPairs7Len","\x08\x00"),
1552                ("NTLMSSPNTLMChallengeAVPairs7UnicodeStr","\xc0\x65\x31\x50\xde\x09\xd2\x01"),
1553                ("NTLMSSPNTLMChallengeAVPairs6Id","\x00\x00"),
1554                ("NTLMSSPNTLMChallengeAVPairs6Len","\x00\x00"),
1555        ])
1556
1557
1558        def calculate(self):
1559                ###### Convert strings to Unicode
1560                self.fields["NTLMSSPNtWorkstationName"] = self.fields["NTLMSSPNtWorkstationName"].encode('utf-16le')
1561                self.fields["NTLMSSPNTLMChallengeAVPairsUnicodeStr"] = self.fields["NTLMSSPNTLMChallengeAVPairsUnicodeStr"].enc
```

Responder/packets.py at bd2e4b5bc7b4ffcc6a7f8c239a0a945c2c822041 · mame82/Responder

WIN-PRH492RQAFV string present within a modified version of Responder on GitHub.

Responder was released in January 2014. It is described as follows in its README file listed on the official GitHub repository: "Responder is an LLMNR, NBT-NS, and MDNS poisoner. It will answer to specific NBT-NS (NetBIOS Name Service) queries based on their name suffix (see: http://support.microsoft.com/kb/163409). By default, the tool will only answer to File Server Service request, which is for SMB. The concept behind this is to target our answers, and be stealthier on the network ..."

Malicious use of Responder was first publicly documented on August 11, 2017 as being used by APT28, also known as Fancy Bear. The tool was used against hotel visitors to spoof NetBios resources. Victims were coerced into connecting to UDP port 137 and disclosing credentials over SMB to APT28, which the threat actor then used to gain elevated access to the network.

More Lessons From Russia: SMB Credential Harvesting Using "file://" Path

Building on the use of Responder, the threat actor also appeared to borrow techniques originating from a different Russian threat actor, Dragonfly, also known as Energetic Bear or Crouching Yeti.

The path "file://82.118.242[.]243/[REDACTED]" used in the spearphish was likely to steal SMB credentials by creating an invisible image tag that the host attempts to fetch over SMB, while giving the attackers a hashed value of the user's NTLM password. When executing the code, the browser creates an invisible image tag and sets the URL to an attack server using the "file://" protocol scheme, which also transmits the user's login NTLM hash. This created an effective watering hole to fingerprint potential victims and gather credentials for subsequent incursions into target networks.

This technique of leveraging the "file://" path to trigger an SMB connection was first publicly detailed by US-CERT on March 15, 2018 as a sophisticated technique used by Russian government actors believed to be the Dragonfly threat actor, targeting the energy industry and other critical infrastructure sectors.

SWC Hosted On 82.118.242[.]243?

Registration details for 82.118.242[.]243, the IP associated with the SMB credential theft detailed above, proved to be inconclusive. WHOIS referenced the IP within a massive range registered to the U.K. ISP Virgin Media (82.0.0.0 - 82.47.255.255). However, MaxMind resolved the IP to Bulgarian hosting provider Histate Global Corp.

Based on the listed vulnerabilities in Shodan and scan results for the machine, 82.118.242[.]242 is a web server likely running Windows Internet Information Services (IIS) 7.5. It has ports 22, 80, 88, 443, 445, 587, 902, and 5985 open.

CVE	Affected Software
CVE-2010-1256	Microsoft IIS 6.0, 7.0, and 7.5
CVE-2010-1899	Microsoft IIS 5.1, 6.0, 7.0, and 7.5
CVE-2010-2730	Microsoft IIS 7.5
CVE-2010-3972	Microsoft FTP Service 7.0 and 7.5 for IIS 7.0 and IIS 7.5
CVE-2012-2531	Microsoft IIS 7.5
CVE-2012-2532	Microsoft FTP Service 7.0 and 7.5 for IIS
CVE-2017-15906	OpenSSH pre-7.6

Vulnerabilities likely associated with 82.118.242[.]243.

Another IP address that falls within the same /24 CIDR range, 82.118.242[.]124, was flagged in Recorded Future with an abnormally high risk score of 89 in July 2018. This was due to the IP appearing in the IOC listing by Cisco Talos as second-stage malware associated with the VPNFilter botnet. This botnet has been attributed to APT28 by the U.S. Department of Justice.

Based on the vulnerability of the web server 82.118.242[.]243 and the use of the “file://” SMB credential stealing technique directing the victim to the IP, we believe the threat actor compromised the web server and used it as a targeted watering hole to illicitly acquire SMB credentials from victims during this campaign.

WIN-AB2I27TG6FK and Chinese Threat Actor TEMP.Periscope

Hostname WIN-AB2I27TG6FK was observed as the NetBios server name of the device sending the spearphish from the VPN IP 193.180.255[.]2.

Open source research for the hostname WIN-AB2I27TG6FK revealed an open directory (Google cached link) at the URL scsnewstoday[.]com/news/ that hosted several files containing the hostname in the filename (see snapshot of the domain below). The domain was previously reported as a C2 used by the Chinese threat actor TEMP.Periscope to deliver their AIRBREAK downloader. AIRBREAK, also known as Orz, is a JavaScript-based backdoor that retrieves commands from hidden strings in compromised webpages and actor-controlled profiles on legitimate services.

File listing on an open directory hosted at http://scsnewstoday[.]com/news.

In addition to AIRBREAK, the scsnewstoday C2 server reportedly hosted other malware and logs relating to TEMP.Periscope malicious activity that targeted Cambodian entities in the run-up to the country's elections. The spearphish against the U.K. engineering company occurred at the same time this campaign was active — in early July 2018. Judging from the naming convention employed on filenames in the open directory, C2S and S2C likely relate to client-to-server and server-to-client connections with the hostname WIN-AB2I27TG6FK, which we assess is likely to be the hostname associated with the scsnewstoday[.]com C2. We'd expect to see many more files listed if the hostnames in the filenames related to the clients, or victims, targeted by TEMP.Periscope.

The domain scsnewstoday[.]com was hosted on U.S. IP 68.65.123[.]230 and registered to domain hosting service Namecheap until July 11, 2018. Details of the C2 domain were published just a day earlier, which we believe may have unnerved TEMP.Periscope operators, resulting in it being dropped. Unfortunately, the open directory is no longer accessible, which hampered our ability to understand the precise nature of the three files containing the WIN-AB2I27TG6FK hostname.

According to industry reporting, Chinese espionage group TEMP.Periscope has conducted large-scale phishing, intrusion, remote access trojan (RAT), and data exfiltration activity since at least 2013. Targeting has primarily focused on maritime-related entities across multiple industries, including engineering, shipping and transportation, manufacturing, defense, government offices, and research universities. However, the group has also targeted professional and consulting services, high-tech industry, healthcare, and media and publishing.

Originating IP for Spearphish 193.180.255[.]2

This IP appeared in the email header information as the X-Forwarded-For IP, indicating that it was the originating IP address for the sender of the spearphish. WHOIS registration data revealed that 193.180.255[.]2 is registered to Privat Kommunikation Sverige AB, which is the full company name of PrivateVPN, a popular commercial VPN service. The company states that they support OpenVPN over TCP/UDP, L2TP, IPSEC, PPTP, and IKEv2 protocols.

Recorded Future identified three VPN connections involving the 193.180.255[.]2 IP between June 30 and July 1, 2018. All three connections were over UDP 500 (IKE/IKEv2), originating from Bangladesh IP 103.198.138[.]187.

Additionally, between July 3 and July 10, 2018, 193.180.255[.]2 established SSH (TCP 22), NetBios (TCP 139), and Microsoft SMB (TCP 445) connections to the malicious SMB credential harvesting C2 82.118.242[.]243. Interestingly, these connections took place during the seven-day window within which the spearphish was sent.

Historic Targeting of U.K. Engineering Company by TEMP.Periscope

Prior to this attempt in July, the same U.K. engineering company had previously been targeted in May 2017. This campaign used the ETERNALBLUE exploit and a unique DNS tunneler backdoor. The DNS tunneler used in the attack was configured to communicate with a subdomain of thyssenkrupp-marinesystems[.]org. The domain was clearly spoofing German defense contractor ThyssenKrupp Marine Systems, which specializes in marine engineering. In addition to hosting the spoofed domain, Netherlands-based HostSailor VPS IP 185.106.120[.]206 also hosted an open directory containing malware and tools for use by the threat actor, not dissimilar to the TEMP.Periscope scsnewstoday[.]com C2 and open directory set up.

Recorded Future analysis on the spoofed domain revealed that this server hosted the SeDll Javascript loader SHA256: 146aa9a0ec013aa5bdba9ea9d29f59d48d43bc17c6a20b74bb8c521dbb5bc6f4, which had been used in August 2017 by Leviathan (also known as TEMP.Periscope) to execute another Javascript backdoor, AIRBREAK. Crucially, the first mention of Leviathan as a Chinese threat actor occurred in October 2017, meaning TEMP.Periscope was using the same infrastructure to target the U.K. engineering company six months earlier.

In November 2017, another spearphish leveraging Microsoft Equation Editor vulnerability CVE-2017-11882 was sent to the U.K. engineering company. This attack delivered a Cobalt Strike payload.

Conclusions and Outlook

The attempted spearphish has revealed a suite of TTPs that are linked to the recent activities of several different threat actors: APT28, Dragonfly, and TEMP.Periscope. We have listed the key TTPs observed in this attack in a chronological format in order to draw attention to the likelihood of techniques being copied from publicly disclosed reporting of these TTPs. These are summarized in the table below:

Observed TTP	TTP Category	Similarity With Historic APT TTPs	Date TTP Publicized
Use of Chinese email client Foxmail	Infrastructure	Previously reported as being a client used by Chinese APT group Luckycat.	2012
Use of open source tool Responder (albeit a modified instance in this case, based on the presence of the hardcoded hostname, WIN-PRH492RQAFV	Malware/ Tooling	APT28 deployed Responder on a hospitality sector network they compromised using ETERNALBLUE. Responder was used to facilitate NetBios poisoning to steal victim credentials.	August 11, 2017
Use of path "file://" in the malicious link provided in the spearphish to harvest SMB credentials	Malware/ Tooling	U.S. NCCIC reported Russian group, Dragonfly, employed watering holes where Javascript code used a hidden iFrame to generate a "file://" connection to a remote server, resulting in an SMB transfer of the victims' NT Local Area Network Manager (NTLM) hash.	March 15, 2018
Spearphish sent to U.K. engineering company email accounts	Victim	The targeting of maritime engineering companies has recently been reported as having been conducted by Chinese APT TEMP.Periscope.	TEMP.Periscope targeting of maritime engineering company on March 16, 2018
WIN-AB2I27TG6FK hostname of device sending spearphish	Infrastructure	Appears in the filename of three separate files listed in the open directory, scsnewstoday[.]com, and used recently by Chinese APT TEMP.Periscope.	July 10, 2018
Spearphish sent to an email possibly belonging to a Cambodian journalist	Victim	Targeting of Cambodian entities has been reported as a known TTP of TEMP.Periscope.	July 10, 2018

Summary of observed TTPs used in attacks and links to similar APT TTPs.

Given that most of the listed APT28, Dragonfly, and TEMP.Periscope TTPs have already been published, we believe there are three likely scenarios for the activity observed:

1. A Russian threat actor was responsible and borrowed TEMP.Periscope TTPs.
2. TEMP.Periscope was responsible and borrowed Russian threat actor TTPs.
3. Another threat actor was responsible that used TTPs from the Russian groups and TEMP.Periscope.

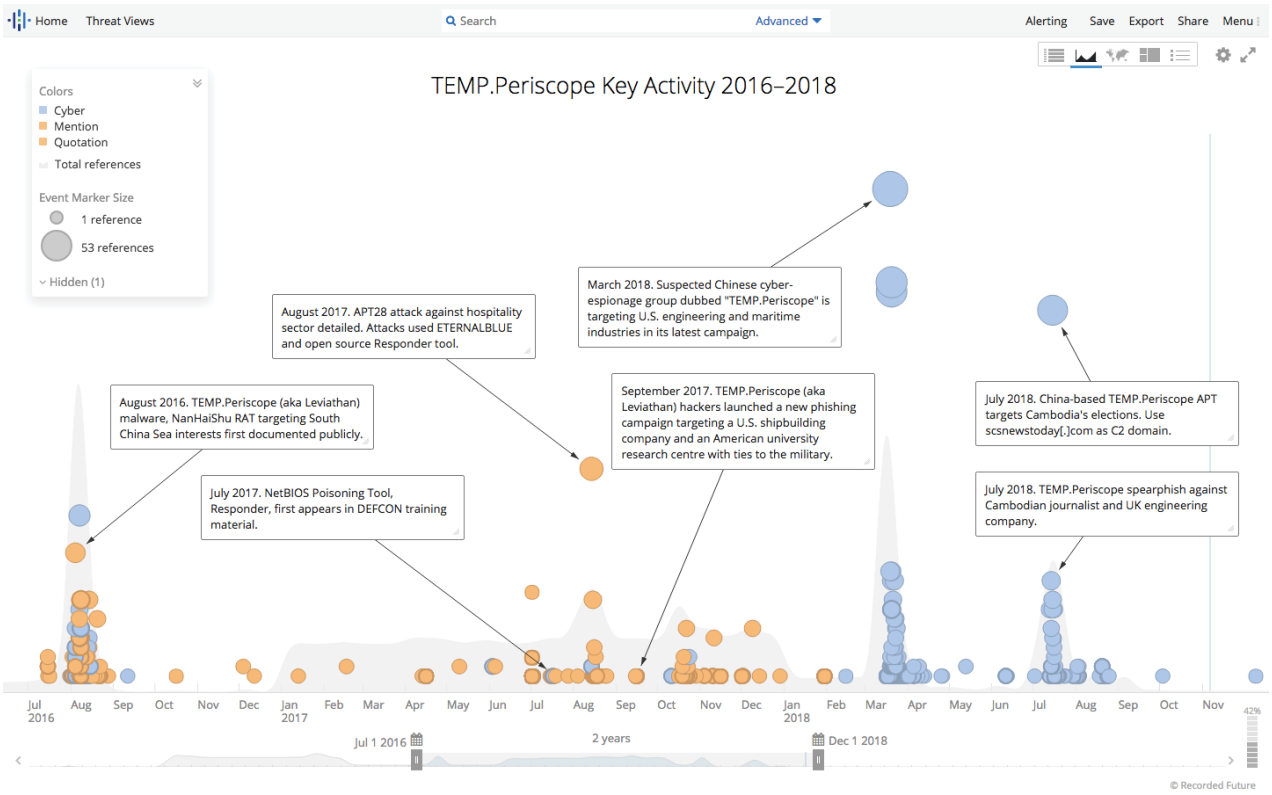
In order to assess which of the three hypotheses above best explains our observations, we assessed the accumulated evidence detailed in this report.

First, we are certain that the attacker used IP 193.180.255[.]2 as a VPN endpoint to send the spearphish because the IP address resolves to Swedish VPN service PrivateVPN. We are also certain that the device that sent the spearphish was associated with the WIN-AB2I27TG6FK hostname. Further, we can state that this hostname was used in the filename of several files hosted on a known TEMP.Periscope C2, which had an open directory. As outlined earlier in this report, we believe the sender of the spearphish, WIN-AB2I27TG6FK, is probably the hostname of the TEMP.Periscope open directory hosted at scsnewstoday[.]com.

The spearphish was sent on July 6, 2018. Just a few days later, FireEye reported on a TEMP.Periscope campaign targeting the Cambodian elections in July 2018 that used the open directory hosted on scsnewstoday[.]com as a C2. The report noted that the same infrastructure was likely active since at least April 2017.

Secondly, the “file://” path included in the spearphish linking to the C2 82.118.242[.]243 was designed to steal credentials over SMB. This technique was documented publicly as a Dragonfly threat actor TTP by the US-CERT in March 2018, almost four months before the observed attack.

The observed hostname on the 82.118.242[.]243 IP was WIN-PRH492RQAFV, which we found was hard coded in a forked Responder script on GitHub. The original Responder script has previously been used by another Russian threat actor, APT28, according to reporting published in August 2017.



Timeline of selected APT28, Dragonfly, and TEMP.Periscope TTP disclosures and activity.

TEMP.Periscope has been actively followed by the research community since at least October 2017 — two months after APT28's use of Responder was disclosed by FireEye in August 2017.[2] There has since been a flurry of reporting on TEMP.Periscope activity in 2018, with campaigns against American and European maritime engineering companies and the Cambodian government. We should note here that the spearphish we observed was also sent to an email account that contained the name of a journalist based in Cambodia and was sent from an account spoofing an Australian journalist that had previously reported on Cambodian topics.

[2] F-Secure published research in August 2016 on their investigations into the NanHaiShu RAT, which has since been attributed to TEMP.Periscope (Leviathan).

Therefore, it is plausible that, with the timeline of Russian tooling being made public prior to the disclosure of the TEMP.Periscope campaigns, TEMP.Periscope adapted their TTPs to either hinder attribution efforts or to simply use techniques that they deemed would be effective.

The overlap in infrastructure with the scsnewstoday[.]com C2 domain is also key; the domain was publicly reported by FireEye as being used by TEMP.Periscope only a few days after the spearphish to the U.K. engineering company was sent, making it highly unlikely that another threat actor could have compromised the C2. Additionally, the longer-term targeting of the U.K. engineering company by TEMP.Periscope since at least May 2017 highlights the group's persistence in attempting to gain access.

Based on the available data and evidence outlined in this report, Recorded Future assesses with medium confidence that Chinese threat actor TEMP.Periscope reused TTPs from other threat groups to target the U.K. engineering company, likely to gain access to their sensitive and proprietary technologies and data. TEMP.Periscope has demonstrated an ability to rapidly adapt its TTPs to learn from other groups, such as APT28 and Dragonfly, either to increase their chances of success in gaining access to the victim network or to obfuscate attribution attempts.

Recorded Future expects TEMP.Periscope to continue to target organizations in the high-tech defense and engineering sectors. The Chinese strategic requirement to develop advanced technology, particularly in marine engineering, remains an intense focus as China looks to dominate the South China Sea territory. We believe TEMP.Periscope will continue to use commodity malware because it is still broadly successful and relatively low cost for them to use. They will continue to observe "trending" vulnerabilities to exploit and use techniques that have been publicly reported in order to gain access to victim networks.

Finally, Recorded Future believes that threat actors are actively emulating each other, monitoring publications and data sources both to protect their infrastructure and to observe techniques that rival actors are using. We anticipate that adversaries will continue to plant false flags, either via technical means (as observed in the Olympic Destroyer campaign) or with technique emulation. As means of detection have drastically improved, the public identification of code overlap and the mapping of TTPs plays into the hands of well-coordinated operations, which can now make attribution findings murky at best. The samples and techniques named in a report can now rapidly be transposed into new or ongoing campaigns due to the volume of public reporting on these issues. This muddying of the waters allows targeted campaigns to better blend in with the noise, attempting to blur the lines between adversary groups.

Network Defense Recommendations

Recorded Future recommends organizations conduct the following measures when defending against TEMP.Periscope's attempts to steal credentials to gain network access:

- Configure your intrusion detection systems (IDS), intrusion prevention systems (IPS), or any network defense mechanisms in place to alert on — and upon review, consider blocking illicit connection attempts from — the external IP addresses and domains listed in Appendix A.
- Include the provided Snort rules in Appendix B in IDS and IPS appliances to detect attempted SMB credential stealing. Also, if applicable, use the provided Bro queries in Appendix B to hunt for signs of TEMP.Periscope TTPs detailed in this report on your network.
- Use Recorded Future's API to import indicators listed in this report (Appendix A) into your endpoint detection and response (EDR) platform.
- Configure endpoint detection and response traffic to alert and block connections to indicators in Appendix A.
- Utilize the provided Yara rule in Appendix C to search your network for evidence of the spearphish being sent to your organization.
- Monitor and restrict SMB traffic across your network, particularly external attempts to authenticate via SMB.

Appendix A — Indicators of Compromise

IPv4
82.118.242[.]243
193.180.255[.]2
185.106.120[.]206
68.65.123[.]230

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

SHA256
146aa9a0ec013aa5bdba9ea9d29f59d48d43bc17c6a20b74bb8c521dbb5bc6f4

Appendix B — Network Monitoring

```
Snort Rules to Detect SMB Credential Snarf (via US-CERT)

alert tcp any any -> any 445 (msg:"SMB Client Request contains 'AME_ICON.
PNG' (SMB credential harvesting)"; sid:42000003; rev:1; flow:established,to_
server; content:"|FF|SMB|75 00 00 00 00|"; offset:4; depth:9; content:"|08
00 01 00|"; distance:3; content:"|00 5c 5c|"; distance:2; within:3; con-
tent:"|5c|AME_ICON.PNG"; distance:7; fast_pattern; classtype:bad-unknown;
metadata:service netbios-ssn;)
-----------------------------------------

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"HTTP URI OPTIONS
contains '/ame_icon.png' (SMB credential harvesting)"; sid:42000004; rev:1;
flow:established,to_server; content:"/ame_icon.png"; http_uri; fast_pat-
tern:only; content:"OPTIONS"; nocase; http_method; classtype:bad-unknown;
metadata:service http;)
-----------------------------------------

alert tcp $EXTERNAL_NET [139,445] -> $HOME_NET any (msg:"SMB Server Traffic
contains NTLM-Authenticated SMBv1 Session"; sid:42000006; rev:1; flow:estab-
lished,to_client; content:"|ff 53 4d 42 72 00 00 00 00 80|"; fast_pat-
tern:only; content:"|05 00|"; distance:23; classtype:bad-unknown; meta-
data:service netbios-ssn;)
```

Recorded Future customers and community members familiar with Bro IDS can utilize its features to threat hunt for TEMP.Periscope activity pertaining to the intrusion documented in this research:

Example Bro Command	Pertinent Indicator(s)	Description
cat dns.log | bro-cut query | grep -iE "thyssenkrupp\-marinesystems\.org"	thyssenkrupp-marinesystems[.]org scsnewstoday[.]com	Search DNS queries for calls made from hosts on your network to TEMP.Periscope malicious C2s
cat dns.log | bro-cut -d answers | grep -E "82\.118\.242\.243"	82.118.242[.]243 193.180.255[.]2 185.106.120[.]206 68.65.123[.]230	Search DNS responses for calls made from hosts on your network to TEMP.Periscope malicious infrastructure
cat conn.log |grep -E "82\.118\.242\.243"	82.118.242[.]243 193.180.255[.]2 185.106.120[.]206 68.65.123[.]230	Search Bro connections log for evidence of connections to TEMP.Periscope malicious infrastructure
cat dce_rpc.log |grep "WIN-PRH492RQAFV" cat ntlm.log |grep "WIN-PRH492RQAFV" cat smb_cmd.log |grep "WIN-PRH492RQAFV" cat smb_files |grep "WIN-PRH492RQAFV" cat smb_mapping.log |grep "WIN-PRH492RQAFV"	WIN-PRH492RQAFV	Search Bro SMB logs for evidence of use of specific modified version of Responder used in this campaign

Appendix C — Yara Rules

```
/*
YARA rule to detect spearphish email (.eml) sent by Chinese threat actor
TEMP.Periscope in July 2018.
*/

rule TEMP_Periscope_July2018_Spearphish : email
{
  meta:
        Author = "Insikt Group, Recorded Future"
        TLP = "White"
        Date = "2018-09-22"
        Description ="Rule to identify spearphish sent by Chinese threat actor
TEMP.Periscope during July 2018 campaign”

  strings:
        $eml_1="From:"
        $eml_2="To:"
        $eml_3="Subject:"
   $greeting_1="Dear,"

        $content_1="Melissa Coade" nocase
        $content_2="Below is the Report Website and conatc"
        $content_3="Would yo mind giving me"

        $url_1="file://"
        $url_2="https://drive.google.com/open?"

  condition:
        all of ($eml*) and
        all of ($greeting*) and
        2 of ($content*) and
        2 of ($url*)
}
```

About Recorded Future

Recorded Future arms security teams with the only complete threat intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.